US006005939A

United States Patent [19]

Fortenberry et al.

[11] **Patent Number: 6,005,939**

[45] **Date of Patent: Dec. 21, 1999**

[54] **METHOD AND APPARATUS FOR STORING AN INTERNET USER'S IDENTITY AND ACCESS RIGHTS TO WORLD WIDE WEB RESOURCES**

[75] Inventors: **Keith Neil Fortenberry**, Boca Raton, Fla.; **Herman Rodriquez**, Austin, Tex.

[73] Assignee: **International Business Machines Corporation**, Armonk, N.Y.

[21] Appl. No.: **08/761,256**

[22] Filed: **Dec. 6, 1996**

[51] **Int. Cl.**[6] **H04L 9/00**

[52] **U.S. Cl.** **380/21**, 380/23; 380/30; 380/43; 705/64; 705/67; 705/76; 713/155; 713/156; 713/167, 713/171; 713/182; 713/185; 713/200

[58] **Field of Search** 380/21, 3, 4, 49

[56] **References Cited**

U.S. PATENT DOCUMENTS

5,081,678	1/1992	Kaufman et al.	380/21
5,452,433	9/1995	Nihart et al.	395/500
5,455,953	10/1995	Russell	395/739
5,463,690	10/1995	Crandall	380/30
5,623,546	4/1997	Hardy et al.	380/4
5,671,279	9/1997	Elgamal	380/23
5,719,942	2/1998	Aldred et al.	380/49
5,724,423	3/1998	Khello	380/23
5,737,414	4/1998	Walker et al.	280/4
5,737,422	4/1998	Billings	380/25
5,784,463	7/1998	Chen et al.	380/21
5,835,595	11/1998	Fraser et al.	380/25
5,852,666	12/1998	Miller et al.	380/4

FOREIGN PATENT DOCUMENTS

0646857	9/1994	European Pat. Off.	G06F 3/033

OTHER PUBLICATIONS

"*IPv6: The New Internet Protocal*," IEEE Communications Magazine, William Stallings, Jul. 1996, pp. 96–108.

Schneier's Applied Cryptography, 2nd Edition, Oct. 1995.

Primary Examiner—Tod R. Swann

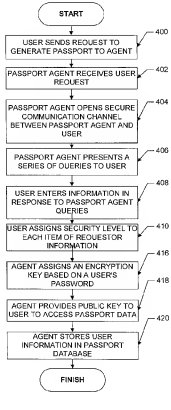
Assistant Examiner—Paul E. Callahan

Attorney, Agent, or Firm—Kudirka & Jobse, LLP

[57] **ABSTRACT**

A method and apparatus for obtaining user information to conduct secure transactions on the Internet without having to re-enter the information multiple times is described. The method and apparatus can also provide a technique by which secured access to the data can be achieved over the Internet. A passport containing user defined information at various security levels is stored in a secure server apparatus, or passport agent, connected to computer network. A user process instructs the passport agent to release all or portions of the passport to a recipient node and forwards a key to the recipient node to unlock the passport information.

19 Claims, 6 Drawing Sheets



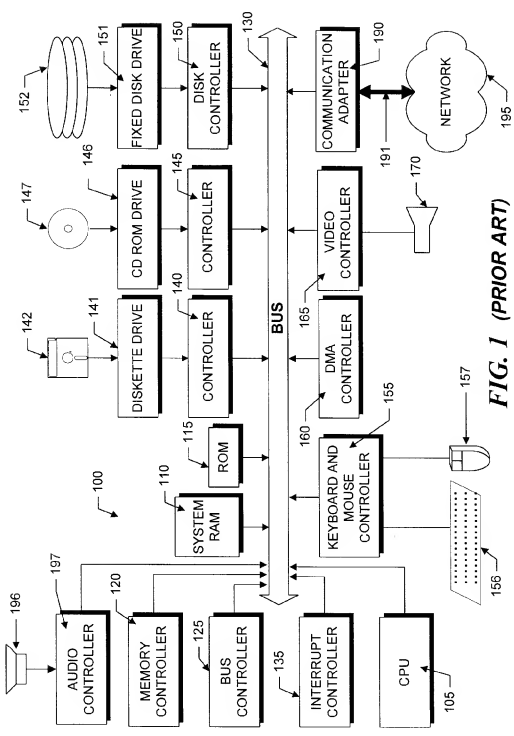


FIG. 1 (PRIOR ART)

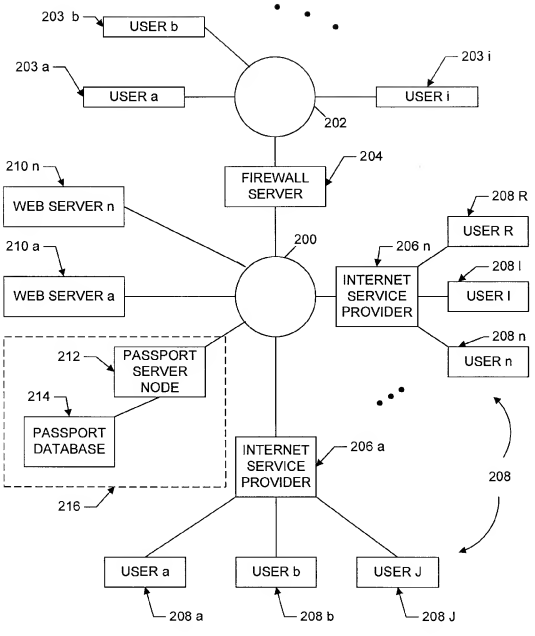

203 b
USER b
203 a
USER a
203 i
USER i
202
210 n
WEB SERVER n
FIREWALL SERVER
204
208 R
USER R
210 a
WEB SERVER a
200
206 n
INTERNET SERVICE PROVIDER
208 I
USER I
208 n
USER n
212
PASSPORT SERVER NODE
214
PASSPORT DATABASE
216
INTERNET SERVICE PROVIDER
206 a
208
USER a
USER b
USER J
208 a
208 b
208 J

FIG. 2A

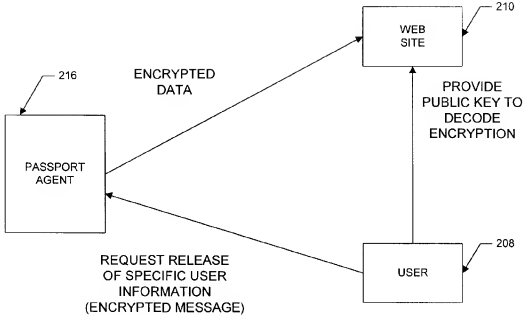

210
WEB SITE
216
ENCRYPTED DATA
PROVIDE PUBLIC KEY TO DECODE ENCRYPTION
PASSPORT AGENT
208
USER
REQUEST RELEASE OF SPECIFIC USER INFORMATION (ENCRYPTED MESSAGE)

FIG. 2B

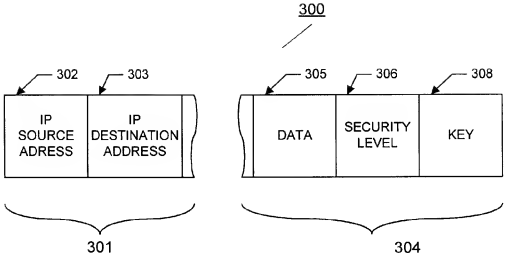

300
302
303
305
306
308
IP SOURCE ADRESS
IP DESTINATION ADDRESS
DATA
SECURITY LEVEL
KEY
301
304

FIG. 3

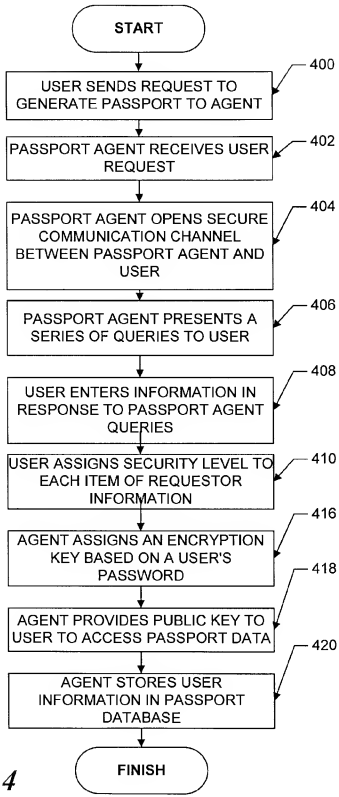

START
USER SENDS REQUEST TO GENERATE PASSPORT TO AGENT
400
PASSPORT AGENT RECEIVES USER REQUEST
402
PASSPORT AGENT OPENS SECURE COMMUNICATION CHANNEL BETWEEN PASSPORT AGENT AND USER
404
PASSPORT AGENT PRESENTS A SERIES OF QUERIES TO USER
406
USER ENTERS INFORMATION IN RESPONSE TO PASSPORT AGENT QUERIES
408
USER ASSIGNS SECURITY LEVEL TO EACH ITEM OF REQUESTOR INFORMATION
410
AGENT ASSIGNS AN ENCRYPTION KEY BASED ON A USER'S PASSWORD
416
AGENT PROVIDES PUBLIC KEY TO USER TO ACCESS PASSPORT DATA
418
AGENT STORES USER INFORMATION IN PASSPORT DATABASE
420
FINISH

FIG. 4

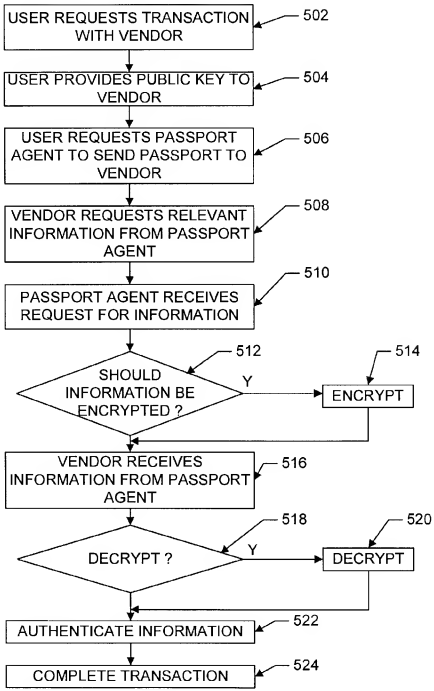

USER REQUESTS TRANSACTION WITH VENDOR
502
USER PROVIDES PUBLIC KEY TO VENDOR
504
USER REQUESTS PASSPORT AGENT TO SEND PASSPORT TO VENDOR
506
VENDOR REQUESTS RELEVANT INFORMATION FROM PASSPORT AGENT
508
PASSPORT AGENT RECEIVES REQUEST FOR INFORMATION
510
SHOULD INFORMATION BE ENCRYPTED ?
512
Y
ENCRYPT
514
VENDOR RECEIVES INFORMATION FROM PASSPORT AGENT
516
DECRYPT ?
518
Y
DECRYPT
520
AUTHENTICATE INFORMATION
522
COMPLETE TRANSACTION
524

FIG. 5

METHOD AND APPARATUS FOR STORING AN INTERNET USER'S IDENTITY AND ACCESS RIGHTS TO WORLD WIDE WEB RESOURCES

FIELD OF THE INVENTION

This invention relates generally to accessing public networks and, more particularly, to a method and apparatus for allowing access to an Internet web site.

BACKGROUND OF THE INVENTION

As is known in the art, there is a trend to conduct business over public computer networks. For example, a user may want to make a purchase or conduct a transaction over a public computer network such as the Internet. To do so, the user accesses the public network through a network node (e.g. a web site) and makes a purchase/transaction request with a particular vendor who is also coupled to the public network via a web site. In response to the user requests, a vendor may request user information such as user name, address, social security number, credit card number, etc.

To continue the transaction, the user responds to the vendor by entering the requested information (e.g. name, address, social security number, credit card number, etc. . . .) at the web site and transmitting the information to the vendor. After receiving the information, the vendor then completes the transaction.

One problem with this approach, however, is that if a user wants to make additional transactions or requests, the user is often required to re-enter the same information for each request. This can lead to mistakes being made in entering the information. This is true even if the information only needs to be entered once in response to a single request. Furthermore, there may be problems maintaining particularly sensitive user information (e.g. credit card number, social security number, etc.) in secret.

For example, to access information on an Internet home page (e.g. the IBM home page on the Internet), a user must specify via a menu selection the language (e.g. English, French, German, etc. . . .) in which the user would like to communicate. Such information must be re-entered each time the same user accesses the IBM home page.

It would therefore be desirable to provide a technique for allowing a user to specify particular information once and have the information be used each time the user accesses any site on the public network.

SUMMARY OF INVENTION

In accordance with the present invention, a passport system includes a single repository of user information in a single format and a passport access provider for accessing the user information in the repository and for providing a user passport to a requestor. With this particular arrangement a consistent, secure and redundancy free technique for obtaining and maintaining user information at one or several sites on a public network is provided. The public network may correspond, for example, to the Internet and the sites may correspond to web sites on the Internet. The consistency, security and redundancy problems are overcome by encapsulating and integrating the user information into the single repository, storing the information in a single format and providing access to that information using a standard interface.

In accordance with a further aspect of the present invention, a method for establishing a passport includes the steps of (a) receiving, in a passport agent, a request from a user to establish a passport, (b) opening a secure communication channel between the passport agent and the user, (c) presenting, via the passport agent, a series of menus to the user in response to which the user enters information and (d) storing the user information as a passport in a passport database. With this particular arrangement, a method for allowing a user to access a plurality of public network sites is provided. In one embodiment, the method further includes the step of securing the passport data. For example, such a method may include the steps of assigning an encryption key to the user and transmitting a public key to the user to allow the user to release a passport from the database. Any particular site which requires particular user information can obtain the user information from the user's passport without having to prompt the user for the parameter each time the web site is visited. To protect the user's privacy, the method may optionally include the steps of assigning a particular security level to each item of user information stored in the passport. By assigning a security level a user can protect sensitive information from being indiscriminately disclosed while the passport still can be used to grant access to more public information. For example, if currently visiting the IBM home page on the Internet, the user must specify a language in which to communicate. Such a user parameter may now be specified in a user passport which is provided to the home page server. Thus, a user need no longer specify such a parameter.

BRIEF DESCRIPTION OF THE DRAWINGS

The above and other features, objects and advantages of the invention will be better understood by referring to the following detailed description in conjunction with the accompanying drawing in which:

FIG. **1** is a block diagram of a computer system suitable for use with the present invention;

FIG. **2A** is a schematic block diagram of a passport agent coupled to an Internet;

FIG. **2B** is a conceptual schematic diagram of the interaction of a user system, passport agent server, and a vendor web site, in accordance with the present invention;

FIG. **3** is a diagrammatical representation of a passport packet;

FIG. **4** is a flow diagram illustrating the steps to register information in a passport agent; and

FIG. **5** is a flow diagram illustrating the steps in completing a transaction between a user and a vendor over an Internet using a passport.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

FIG. **1** illustrates the system architecture for a computer system **100** such as an IBM PS/2®, on which the invention may be implemented. The exemplary computer system of FIG. **1** is for descriptive purposes only. Although the description may refer to terms commonly used in describing particular computer systems, such as in IBM PS/2 computer, the description and concepts equally apply to other systems, including systems having architectures dissimilar to FIG. **1**.

Computer system **100** includes a central processing unit (CPU) **105**, which may be implemented with a conventional microprocessor, a random access memory (RAM) **110** for temporary storage of information, and a read only memory (ROM) **115** for permanent storage of information. A memory controller **120** is provided for controlling RMA **110**.

A bus **130** interconnects the components of computer system **100**. A bus controller **125** is provided for controlling bus **130**. An interrupt controller **135** is used for receiving and processing various interrupt signals from the system components.

Mass storage may be provided by diskette **142**, CD ROM **147**, or hard drive **152**. Data and software may be exchanged with computer system **100** via removable media such as diskette **142** and CD ROM **147**. Diskette **142** is insertable into diskette drive **141** which is, in turn, connected to bus **30** by a controller **140**. Similarly, CD ROM **147** is insertable into CD ROM drive **146** which is, in turn, connected to bus **130** by controller **145**. Hard disk **152** is part of a fixed disk drive **151** which is connected to bus **130** by controller **150**.

User input to computer system **100** may be provided by a number of devices. For example, a keyboard **156** and mouse **157** are connected to bus **130** by controller **155**. An audio transducer **196**, which may act as both a microphone and a speaker, is connected to bus **130** by audio controller **197**, as illustrated. It will be obvious to those reasonably skilled in the art that other input devices, such as a pen and/or tabloid may be connected to bus **130** and an appropriate controller and software, as required. DMA controller **160** is provided for performing direct memory access to RAM **110**. A visual display is generated by video controller **165** which controls video display **170**. Computer system **100** also includes a communications adaptor **190** which allows the system to be interconnected to a local area network (LAN) or a wide area network (WAN), schematically illustrated by bus **191** and network **195**.

Operation of computer system **100** is generally controlled and coordinated by operating system software, such as the OS/2® operating system, available from International Business Machines Corporation, Boca Raton, Fla. The operating system controls allocation of system resources and performs tasks such as processing scheduling, memory management, networking, and I/O services, among things.

In one embodiment, the passport methods of the present invention are implemented in the C++ programming language using object-oriented programming techniques. C++ is a compiled language. That is, programs are written in a human-readable script and this script is then provided to another program called a compiler which generates a machine-readable numeric code that can be loaded into, and directly executed by, a computer.

As described below, the C++ language has certain characteristics which allow a software developer to easily use programs written by others while still providing a great deal of control over the reuse of programs to prevent their destruction or improper use. The C++ language is well known and many articles and texts are available which describe the language in detail. In addition, C++ compilers are commercially available from several vendors including Borland International, Inc. and Microsoft Corporation. Accordingly, for reasons of clarity, the details of the C++ language and the operations of the C++ compiler will not be discussed further in detail herein.

As will be understood by those skilled in the art, Object-Oriented Programming (OOP) techniques involve the definition, creation, use and destruction of "objects." Objects are software entities comprising data elements, or attributes, and methods, or functions, which manipulate the data elements. The attributes and related methods are treated as a single entity and can be created, used and deleted as if they were a single item. Together, the attributes and methods enable objects to model virtually any real-world entity in terms of its behavior, which can be represented by its data manipulation functions. In this way, objects can model concrete things like people and computers, and they can also model abstract concepts like numbers or geometrical designs.

Objects are defined by creating "classes" which are not objects themselves, but which act as templates that instruct the compiler how to construct the actual object. A class may, for example, specify the number and type of data variables and the steps involved in the methods which manipulate the data. When an object-oriented program is compiled, the class code is compiled into the program, but no objects exist. Therefore, none of the variables or data structures in the compiled program exist or have any memory allotted to them. An object is actually created by the program at runtime by means of a special function called a constructor which uses the corresponding class definition and additional information, such as arguments provided during object creation, to construct the object. Likewise objects are destroyed by a special function called a destructor. Objects may be used by using their data and invoking their functions. When an object is created at runtime memory is allotted and data structures are created.

The principle benefits of object-oriented programming techniques arise out of three basic principles; encapsulation, polymorphism and inheritance. More specifically, objects can be designed to hide, or encapsulate, all, or a portion of, the internal data structure and the internal functions. More particularly, during program design, a program developer can define objects in which all or some of the attributes and all or some of the related functions are considered "private" or for use only by the object itself. Other data or functions can be declared "public" or available for use by other programs. Access to the private variables by other programs can be controlled by defining public functions for an object which access the object's private data. The public functions form a controlled and consistent interface between the private data and the "outside" world. Any attempt to write program code which directly accesses the private variables causes the compiler to generate an error during program compilation which errors stops the compilation process and prevents the program from being run.

Polymorphism is a concept which allows objects and functions which have the same overall format, but which work with different data, to function differently in order to produce consistent results. For example, an addition function may be defined as variable A plus variable B (A+B) and this same format can be used whether the A and B are numbers, characters or dollars and cents. However, the actual program code which performs the addition may differ widely depending on the type of variables that comprise A and B. Polymorphism allows three separate function definitions to be written, one for each type of variable (numbers, characters, and dollars). After the functions have been defined, a program can later refer to the addition function by its common format (A+B) and, at runtime, the program will determine which of the three functions is actually called by examining the variable types. Polymorphism allows similar functions which produce analogous results to be "grouped" in the program source code to produce a more logical and clear program flow.

The third principle which underlies object-oriented programming is inheritance, which allows program developers to easily reuse pre-existing programs and to avoid creating software from scratch. The principle of inheritance allows a software developer to declare classes (and the objects which are later created from them) as related. Specifically, classes

may be designated as subclasses of other base classes. A subclass "inherits" and has access to all of the public functions of its base classes just as if these function appeared in the subclass. Alternatively, a subclass can override some or all of its inherited functions or may modify some or all of its inherited functions merely by defining a new function with the same form (overriding or modification does not alter the function in the base class, but merely modifies the use of the function in the subclass). The creation of a new subclass which has some of the functionality (with selective modification) of another class allows software developers to easily customize existing code to meet their particular needs.

Referring now to FIG. 2A, a public network or internet **200** is coupled to a private network **202** through a fire wall server **204**. As used herein, the term "internet" generally refers to any collection of distinct networks working together to appear as a single network to a user. The term "Internet", on the otherhand, refers to the so-called world wide "network of networks" that are connected to each other using the Internet protocol (IP) and other similar protocols. The Internet provides file transfer, remote log in, electronic mail, news and other services.

As described herein, the exemplary public network of FIG. 2A is for descriptive purposes only. Although the description may refer to terms commonly used in describing particular public networks such as the Internet, the description and concepts equally apply to other public and private computer networks, including systems having architectures dissimilar to that shown in FIG. 2A.

One of the unique aspects of the Internet system is that messages and data are transmitted through the use of data packets "data grams." In a data gram based network messages are sent from a source to a destination in a similar manner to a government mail system. For example, a source computer may send a data gram packet to a destination computer regardless of whether or not the destination computer is currently online and coupled to the network. The Internet protocol (IP) is completely sessionless, such that IP data gram packets are not associated with one another.

The fire wall server **204** is a computer which couples the computers of a private network e.g. network **202** to the Internet **200** and may thus act as a gatekeeper for messages and data grams going to and from the Internet **200**. An Internet service provider **206** is also coupled to the Internet **200**. A service provider is an organization that provides connections to a part of the Internet. Internet service provider **206** is also a computer which couples a plurality of users **208***a*–**208**N to the Internet **200**. Thus, users **208** are coupled to the Internet through Internet service provider **206**. Also coupled to the Internet in a plurality of web sites or nodes **210***a*–**210***n* generally denoted **210**. When a user wishes to conduct a transaction at one of the nodes **210**, the user accesses the node **210** through the Internet **200**.

Each node in the fire wall shown in FIG. 2A is configured to understand which fire wall and node to send data packets to given a destination IP address. This may be implemented by providing the fire walls and nodes with a map of all valid IP addresses disposed on its particular private network or another location on the Internet. The map may be in the form of prefix matched up to and including the full IP address.

Also coupled to Internet **200** is a passport server **212** and a passport data base **214**. Passport server **212** and passport database **214** may be collectively referred to as a passport agent **216**. Users **208** can store certain personal and optional demographic information in passport database **214**. The information need only be stored once, and, at the user's option, assigned a security level for each item of information. The information may be stored, for example, as a record or as a file. Thus, passport agent **216** includes a database of user information for each of the users who wish to utilize the services of passport agent **216**. The information for each particular user is stored in a particular data structure referred to as a passport.

Passport agent **216** may be provided, for example, as an object-oriented database management system (DBMS), a relational data base management system (e.g. DB2, SQL, etc) or another conventional data base package which includes a security/authenication function. Thus, the database can be implemented using object-oriented technology or via text files which utilize a security system.

Referring now to FIG. 2B, in general overview, the passport system operates in the following manner. User **208** who wishes to conduct a transaction at web site **210** requests that passport agent **216** release specific user information to web site **210**. The request is made as an encrypted message to passport agent **216**. Passport agent **216** has previously been provided a key with which to decrypt the encrypted message from user **208**. Passport agent **216** decrypts the request from user **208** to determine, inter alia, the particular web site to which a passport of the user **208** should be sent.

Passport agent **216** then provides encrypted data to the particular web site here denoted as web site **210**. User **208** has previously provided to web site **210** a public key with which web site **210** can decode the encrypted data provided by passport agent **216**.

The web site **210** receives the encrypted user information (i.e. the passport) from passport agent **216** and unlocks the message using the public key provided by the user **208**. If the web site **210** is unable to unlock any of the environment variables in the passport, the request is ignored, as explained hereinafter.

It should be noted that user **208** can provide to web site **210** one of several public keys which allow web site **210** to unlock data having one of several security levels. For example, user **208** may have a first key which unlocks confidential user information in the user passport, a second key which unlocks secret user information in the user passport and a third key which unlocks top secret user information in the user passport. Thus, to unlock all the data in the passport, user **208** would have to provide to web site **210** all three keys.

Referring now to FIG. **3**, a transmission packet **300** includes a header portion **301**, having IP source address **302** and destination address **303**, and a passport portion **304**, having a data structure which includes fields **305**, **306**, and **308**.

First data field **305** may contain two classes of data. The first class of information corresponds to real information about a user such as the user's real name, address, credit card information, social security number, etc. The real information is typically highly sensitive in nature and is closely guarded by the user. The first class of information is thus typically encrypted and is available only at the user's discretion. As mentioned above in conjunction with FIG. 2B, the user has a public key which the user can provide to others coupled to a network. The holder of the key can decrypt the user information.

The second class of information included in first data field **305** is virtual information. The virtual information is created and selected by the user. Virtual information includes items such as a virtual (i.e. not real) identification that can be used when visiting web sites and other Internet locations, brows-

ing show rooms on the Internet, etc. This information may or may not be encrypted as per the user's wish. Virtual information may thus include information the user perceives not confidential in nature and may include users preferences, tastes, goals for visiting web sites, etc., yet the user may want to consider it private although not confidential. It should be noted that the term "visiting a web site" generally refers to a method of requesting a document from a web server.

At the user's option, virtual information can be converted to real information via a menu selection. In that event, the selected virtual information becomes restricted (e.g. encrypted) and is no longer publicly available to others on the web.

For example, John Doe, a real user at the Internet, chooses to travel the Internet and be known by the name Jane Doe. Further, John Doe wants to present himself through a picture of a site list when visiting an Internet site or when communicating with other users on the Internet. John Doe's passport contains optional information that he is a classical musical buff. Thus, with the passport method, the user is allowed to present himself as the real person he is when required and as a virtual person on occasions where he wants to assume that virtual identity.

The passport **304** includes a second field corresponding to a security level field **306**. A security level is assigned to each item of user information included in the passport data field **305**. Thus, for example, if data in field **305** is assigned a security level of 0 then the data is clear. Alternatively, if the data is assigned a security level of 1 then the data is secured via a security technique such as an encryption technique. The passport **304** also includes a key field **308**. One or more keys for encryption and decryption may be stored in key field **308**.

Referring to FIG. **4**, a flow diagram illustrating the process steps to create a passport is shown. Coding of the process steps of the flowchart of FIG. **4** into instructions suitable to control the computer systems in the passport agent **216** and the user system **208** will be understood by those having ordinary skill in the art of programming. First, the user sends a request to generate a passport to passport agent **216**, as illustrated by process step **400**. The passport agent receives the request, as illustrated by process step **402**, and opens a secure communication channel between the passport agent and the requesting user, as illustrated by process **404**. Passport agent **216** then presents to the user a series of queries which may be in the form of menus, as illustrated by process block **406**. In response, the user enters the requested information such as social security number, drivers license number, etc., and a corresponding level of security to protect the information item, as illustrated by process blocks **408** and **410**. The user specified information is referred to herein as user information or environmental variables. The security levels assigned to each item of user information or environment variables range from highly secure to public. For example, particularly sensitive information may be designated as highly secured and assigned a high security level of 100 on an exemplary scale of 0–100 levels. Less sensitive information may be designated as less secured or even public and assigned a lower security level approaching or equal to zero. Next, passport agent **216** provides a public key to the user to access the passport data, as illustrated by process **418**. Finally, the user's information which collectively comprises the Internet passport is stored and maintained in a highly secured server site on the Internet which serves as the passport agent and guarantees the integrity of the users passport, as illustrated by process block **420**.

Security keys are delivered to the passport requestor also in a secure manner. As mentioned above, several security keys may be given to a user, such that access to information may be granted at various levels such as real-ID (very secure), virtual-ID and less private information classes. In this manner, the passport agent protects the passport information provided by the user.

When the passport agent sends passport information to the web server on behalf of the passport holder, the private key is used to encrypt the specific information authorized by the passport holder. When the vendor's server receives passport data from the passport agent, one of the public keys sent by the user is used to unlock the passport data. If the public key does not unlock the passport data, the vendor's server simply ignores the users request.

A security level is also used to assign an encryption key based on a user's password. The encryption method uses the concept of public and private keys so that the public key is given the user to access passport data and the passport agent presents the encrypted user data based on the private key. No one but the passport agent on the Internet has access to the private key. The passport owner has a copy of the public key.

Referring now to FIG. **5**, a flowchart illustrating the process steps for providing access to a users internet passport via passport agent is illustrated. The coding of the process steps of the flowchart of FIG. **5** into instructions suitable to control passport agent **216**, web site **210** and user **208** will be understood by those ordinary skill in the art of programming. First, the user requests a transaction with a particular vendor, i.e., web site **210**, as illustrated by process block **502**. Next, the user provides a public key to the vendor, as illustrated in process block **504**. The public key was previously provided to the user by passport agent **216**. Next, the user requests that passport agent **216** send the user's passport to the vendor, as illustrated by process block **506**. This message is encrypted with a security key obtained by the user via a secured method. The vendor requests relevant information contained in the user environment variables from the passport agent, as illustrated by process block **508**. The request for information is specified in the message as follows: RELEASE-TYPE TO INTERNET-SITE ON BEHALF OF MY-USER-ID. For example, when requesting the passport agent to release social security number information, the message looks like: RELEASE SOCIAL-SECURITY-NUMBER TO WEB-SITE-X ON BEHALF OF MY-USER-ID. Passport agent **216** receives the request for the information, as illustrated by process block **510** and, based on the security level of the identified information, determines whether or not the requested information should be transmitted to the vendor in encrypted form, as illustrated by decisional block **512**. If the information is to be encrypted, an encryption process is carried out by passport agent **216**, as illustrated by process block **514**.

If the data is encrypted, the private key is used to encrypt the contents of the user environment variables. The encrypted data contains the name of the user environment variable and its assigned value. Otherwise, the requested information is sent to the vendor by passport agent **216**, as illustrated by process block **516**. When the vendor, i.e. the web server receives passport data from the passport agent **216**, and such user information is encrypted, the public key sent by the user is used to unlock and decrypt the passport data, as illustrated by the decisional block **518** and process block **520**. If the public security key does not unlock the passport data, the vendor simply ignores the users request. Next, the users information is authenticated by the vendor, e.g. verified with an on-line financial database etc., in a

manner understood by those reasonably skilled in the arts, as illustrated by process block **522**. Finally, once the information has been authenticated the vendor is able to complete the transaction, as illustrated by process block **524**.

In the exemplary embodiment, both the passport agent and the web site of the vendor subscribe to the protocol which enable them to participate in the passport system contemplated herein. Further, the public and private keys described herein may be encrypted using a double keying encryption technology technique currently known in the art.

As indicated heretofore, aspects of this invention pertain to specific "method functions" implementable on computer systems. Those skilled in the art should readily appreciate that programs defining these functions can be delivered to a computer in many forms; including, but not limited to: (a) information permanently stored on non-writable storage media (e.g., read only memory devices within a computer or CD-ROM disks readable by a computer I/O attachment); (b) information alterably stored on writable storage media (e.g., floppy disks and hard drives); or (c) information conveyed to a computer through communication media such as telephone networks. It should be understood, therefore, that such media, when carrying such information, represent alternate embodiments of the present invention.

Having described preferred embodiments of the invention, it will now become apparent to one of ordinary skill in the art that other embodiments incorporating their concepts may be used.

For example, it should be noted that in the particular embodiment described above in conjunction with FIG. **2**A, passport security is provided via a public key- private key encryption technique. In other embodiments, however, passport security may be provided from other techniques. For example, the system may be made secure by using a so-called SSL system in which, a server is certified with the SSL system and a client browser (e.g. a Netscape browser) establishes a connection with the certified server. Security in the connection is established via methods provided a security system provider such as VeriSign, for example. Thus, in this particular technique, the client browser is provided having the appropriate authentification codes and the browser determines whether it is receiving appropriate verification/authentication signals. Such security may be provided, for example, on a per session basis, on connections established between a client and the certified server. It should also be recognized that other encryption techniques such as the Date Encryption Standard (DES) and the Pretty Good Privacy (PGP) system can also be used.

It is felt therefore that these embodiments should not be limited to disclosed embodiments, but rather should be limited only by the spirit and scope of the appended claims.

What is claimed is:

1. A method of sending data from a first node to a second node utilizing a passport server node having a plurality of passports stored therein, a network comprising and interconnecting the first, second and passport server nodes, each of the plurality of passports having a data portion, a security level, and a key, the method comprising the steps of:

maintaining a passport database for storing profile data for each of a plurality of users in a data structure comprising the passport for the corresponding user, the first node corresponding to a first of the users and to a first of the passports:

transmitting a first request from the first node to the second node for a transaction with the second node;

transmitting a public key from the first node to the second node, the public key having been previously provided by the passport server node to the first node;

transmitting an encrypted message from the first node to the passport server node wherein the encrypted message directs the passport server node to transmit the first passport stored in the passport server node to the second node;

transmitting the first passport from the passport server node to the second node; and

if the data portion of the transmitted first passport is encrypted, the second node decodings via the public key transmitted from the first node to the second node, the data portion of the the first passport so as to use the data portion for the transaction with the first node.

2. The method of claim **1** further comprising the steps of:

receiving the encrypted message in the passport server node; and

decrypting the encrypted message in the passport server node.

3. The method of claim **2**

A) wherein each of the data portions of the passports includes one or more data items comprising profile data, and each of the passports has a security level associated with each of the data items;

B) wherein the message decrypting step includes the step of: extracting a request for a first data item comprising the requested data item from the encrypted message; and

C) wherein the determining step includes the step of: responsive to the decrypted message, and based at least in part on the security level of requested data item, the passport server node determining whether the requested data item of the data portion of the first passport should be transmitted to the second node in encrypted form, and, if so, encrypting the data portion.

4. A computer server apparatus for use with a computer network, the computer server apparatus for transmitting information between two nodes coupled to the computer network, the server apparatus comprising:

means disposed at a user profile node for registering a plurality of user profile information, the user profile information containing multiple data items wherein at least some of the information is encrypted; the user profile information including a security level for accessing each of the data items;

means for storing the user profile information in data structures comprising a plurality of passports each including a plurality of the data items corresponding to a user;

means disposed at the user profile node for receiving an encrypted message from a user, the encrypted message including a request for transmission of data items in a specified one of the passports to a specified address of a destination node on the computer network;

means disposed at the user profile node for decrypting the encrypted message provided by the user; and

means responsive to the request for transmitting said requested data items to the destination node.

5. A system for sending data over a public network, the system comprising:

means for transmitting a first request from a first node to a second node over the public network for a transaction with the second node;

means for transmitting a public key from the first node to the second node over the public network;

a passport server node, coupled to the computer network, said passport server node having a memory for storing

a plurality of passports, each of the passports corresponding to one of a like plurality of users and each of the plurality of passports having a data portion, a security level portion, and a key portion, the data portion of each of the passports having profile data for one of the users the passport server node comprising:

means for receiving an encrypted message transmitted from the first node to the passport server node wherein the encrypted message directs the passport server node to transmit a particular one of the plurality of passports stored in the passport server node to the second node;

means for decrypting the encrypted message in the passport server node and extracting therefrom information identifying the particular passport;

responsive to the message, and based at least in part on the security level of the particular passport, the passport server node determining whether the data portion of the particular passport should be transmitted to the second node in encrypted form, and, if so, encrypting the data portion;

means for transmitting the particular one of the plurality of passports from the passport server node to the second node; and

means in the second node for decoding via the public key transmitted from the first node to the second node, the data portion of the particular one of the plurality of passports if the data portion is encrypted.

6. A method for establishing a user passport for use by the user in connection with transactions over a network with third-party sites, comprising the steps of:

(a) a user sending a request to generate a passport to a passport agent;

(b) receiving the request in the passport agent;

(c) opening, via the passport agent, a secure communication channel between the passport agent and the user;

(d) presenting, via the passport agent, series of queries to the user;

(e) the user entering user profile information, including a plurality of data items regarding the user, in response to the passport agent queries;

(f) the user assigning a security level to each item of user profile information;

(g) the passport agent assigning an encryption key to the user based at least in part on the security level assigned each item of user profile information by the user;

(h) the passport agent transmitting at least one public key, which corresponds to the assigned encryption key, for enabling the user to share the public key with one or more of the third-party sites and thereby enabling the one or more third-party sites to access passport profile information; and

(i) storing the user profile information in a passport database for subsequent transmission and use, responsive to a user request, in connection with transactions with the third-party sites.

7. The method of claim **6** wherein the step (g) comprises:

(g.1) assigning an encryption key based on a password assigned to the user.

8. The method of claim **6** wherein the step (h) comprises:

(h.1) transmitting the public key to the user over the secure communication channel between the passport agent and the user.

9. A system for establishing a user passport comprising:

a passport database for storing a plurality of user passports, each comprising a data structure containing user information with respect to a different one of a plurality of users;

means for receiving a request to generate a passport from a user;

means for establishing a secure communication channel to the user;

means for presenting a query to the user;

means for receiving user information entered in response to the query;

means for assigning a security level to each item of user information received by said means for receiving;

means for assigning an encryption key to the user;

means for storing the user information in one of the passports in said passport database corresponding to the user; and

means for transmitting a public key to the user, which corresponds to the assigned encryption key, for enabling the user to share the public key with one or more third parties and thereby enable the one or more third parties to access the user information stored in the corresponding passport in said passport database.

10. The system of claim **9** wherein the means for assigning an encryption key includes means for assigning an encryption key based on a password assigned to the user.

11. The system of claim **9** wherein the means for transmitting the public key to the user includes means for transmitting the public key to the user over the secure communication channel.

12. The method of claim **3**, wherein the message encrypting step includes the step of encrypting the requested data item using a private key.

13. The method of claim **3**, wherein the step of the transmitting a public key from the first node to the second node includes the steps of ascertaining, based at least in part on the security level of requested data item, which of a plurality of public keys to send to the second node, each of a plurality of the data items having a corresponding key associated with the security level of the data item.

14. The method of claim **1** further comprising the step of authenticating the decoded data portion.

15. The method of claim **4**, wherein, responsive to the encrypted message, and based at least in part on the security level of the first passport, the passport server node determining whether the data portion of the first passport should be transmitted to the second node in encrypted form, and, if so, encrypting the data portion.

16. The computer system of claim **4** further comprising means responsive to the requests for transmitting to the destination node the one passport and a public key corresponding to the security level of the requested data items.

17. A computer program product comprising a computer-readable media, and computer-executable program code stored on the computer-readable media, wherein the program code is suitable for use in a system for sending data from a first node to a second node utilizing a passport server node having a plurality of passports stored therein, each of the plurality of passports having a data portion, a security level, and a key, the program code comprising:

program code for accessing a passport database stored on a passport server node, the passport database storing profile data for each of a plurality of users in a data structure comprising the passport for the corresponding user, the first node corresponding to a first of the users and to a first of the passports;

program code for transmitting a first request from the first node to the second node for a transaction with the second node;

program code for transmitting a public key from the first node to the second node, the public key having been previously provided by the passport server node to the first node; and

program code for transmitting an encrypted message from the first node to the passport server node wherein the encrypted message directs the passport server node to transmit the first passport stored in the passport server node.

18. A computer program product comprising a computer-readable media, and computer-executable program code stored on the computer-readable media, the program code capable of establishing a user passport for use by a user in connection with transactions over a network with third-party sites, the program code comprising:

(a) program code for receiving a request from a user to generate a passport;

(b) program code for presenting a series of queries to the user, and for receiving user profile information from the user, including a plurality of data items regarding the user, in response to the queries;

(c) program code for receiving from the user a security level assigned to each item of user profile information;

(d) program code for assigning an encryption key to the user based at least in part on the security level assigned each item of user profile information by the user;

(e) program code for transmitting at least one public key, which corresponds to the assigned encryption key, for enabling one or more third-party sites to access the passport profile information; and

(f) program code for storing the user profile information in a passport database for subsequent transmission and use, responsive to a user request, in connection with transactions with the third-party sites.

19. A computer data signal embodied in a carrier wave, the computer data signal capable of use in establishing a user passport for use by a user in connection with transactions over a network with third-party sites, the computer data signal comprising:

(a) program code portion for receiving a request from a user to generate a passport;

(b) program code portion for presenting a series of queries to the user, and for receiving user profile information from the user, including a plurality of data items regarding the user, in response to the queries;

(c) program code portion for receiving from the user a security level assigned to each item of user profile information;

(d) program code portion for assigning an encryption key to the user based at least in part on the security level assigned each item of user profile information by the user;

(e) program code portion for transmitting at least one public key, which corresponds to the assigned encryption key, for enabling one or more third-party sites to access the passport profile information; and

(f) program code portion for storing the user profile information in a passport database for subsequent transmission and use, responsive to a user request, in connection with transactions with the third-party sites.

* * * * *

US005960411A

United States Patent [19]

Hartman et al.

[11] **Patent Number: 5,960,411**

[45] **Date of Patent: Sep. 28, 1999**

[54] **METHOD AND SYSTEM FOR PLACING A PURCHASE ORDER VIA A COMMUNICATIONS NETWORK**

[75] Inventors: **Peri Hartman**; **Jeffrey P. Bezos**; **Shel Kaphan**; **Joel Spiegel**, all of Seattle, Wash.

[73] Assignee: **Amazon.com, Inc.**, Seattle, Wash.

[21] Appl. No.: **08/928,951**

[22] Filed: **Sep. 12, 1997**

[51] **Int. Cl.**[6] **G06F 17/60**

[52] **U.S. Cl.** **705/26**; 705/27; 345/962

[58] **Field of Search** 705/26, 27; 380/24, 380/25; 235/2, 375, 378, 381; 395/188.01; 345/962

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,937,863	6/1990	Robert et al.	380/4
5,204,897	4/1993	Wyman	380/4
5,260,999	11/1993	Wyman	384/4
5,627,940	5/1997	Rohra et al.	395/12
5,640,501	6/1997	Turpin	395/768
5,640,577	6/1997	Scharmer	395/768
5,664,111	9/1997	Nahan et al.	705/27
5,715,314	2/1998	Payne et al.	380/24
5,715,399	2/1998	Bezos	705/27
5,727,163	3/1998	Bezos	705/27
5,745,681	4/1998	Levine et al.	395/200.3
5,758,126	5/1998	Daniels et al.	395/500

FOREIGN PATENT DOCUMENTS

0855659 A1	1/1998	European Pat. Off.	G05F 17/30
0855687 A2	1/1998	European Pat. Off.	G07F 19/00
0845747A2	6/1998	European Pat. Off.	G06F 17/60
0883076A2	12/1998	European Pat. Off.	G06F 17/60
WO 95/30961	11/1995	WIPO	G06F 17/60
WO 96/38799	12/1996	WIPO	G06F 17/60
WO 98/21679	5/1998	WIPO	G06F 17/60

OTHER PUBLICATIONS

Jones, Chris. "Java Shopping Cart and Java Wallet; Oracles plans to join e-commerce initiative." Mar. 31, 1997, InfoWorld Media Group.

"Pacific Coast Software Software creates virtual shopping cart." Sep. 6, 1996. M2 Communications Ltd 1996.

"Software Creates Virtual Shopping Cart." Sep. 5, 1996. Business Wire, Inc.

Terdoslavich, William. "Java Electronic Commerce Framework." Computer Reseller News, Sep. 23, 1996, CMP Media, Inc., 1996, pp. 126, http://www.elibrary.com/id/101/101/getdoc . . . rydocid=902269@library_d&dltype=0-0&dinst=. [Accessed Nov. 19, 1998].

"Internet Access: Disc Distributing Announces Interactive World Wide." Cambridge Work-Group Computing Report, Cambridge Publishing, Inc., 1995, http://www.elibrary.com/id/101/101/getdoc . . . docid=1007497@library_a&dltype=0-0&dinst=0. [Accessed Nov. 19, 1998].

(List continued on next page.)

Primary Examiner—James P. Trammell
Assistant Examiner—Demetra R. Smith
Attorney, Agent, or Firm—Perkins Coie LLP

[57] **ABSTRACT**

A method and system for placing an order to purchase an item via the Internet. The order is placed by a purchaser at a client system and received by a server system. The server system receives purchaser information including identification of the purchaser, payment information, and shipment information from the client system. The server system then assigns a client identifier to the client system and associates the assigned client identifier with the received purchaser information. The server system sends to the client system the assigned client identifier and an HTML document identifying the item and including an order button. The client system receives and stores the assigned client identifier and receives and displays the HTML document. In response to the selection of the order button, the client system sends to the server system a request to purchase the identified item. The server system receives the request and combines the purchaser information associated with the client identifier of the client system to generate an order to purchase the item in accordance with the billing and shipment information whereby the purchaser effects the ordering of the product by selection of the order button.

26 Claims, 11 Drawing Sheets

OTHER PUBLICATIONS

Nance, Barry, "Reviews: A Grand Opening for Virtual Storefront With Middleware." Jun. 1, 1997, CMP Media, Inc. 1997, p. 80, http://www.elibrary.com/getdoc.egi?id=117 . . . docid=1257247@library_a&dtype=0–0&dinst=0. [Accessed Nov. 19, 1998].

"Go–Cart Shopping Cart Software Features" 1996 GO International, Inc. http://www.go–cart.com/features.html. [Accessed Nov. 19, 1998].

"PerlShop Manual (version 2.2)." 1996, ARPAnet Corp. http://www.w3u.com/grokksoft/shop/perlman.html. [Accessed Nov. 19, 1998].

"Sax Software Announces Sax NetSell; Sax NetSell's design–time ActiveX controls make Internet commerce easy."1997, Sax Software Corp.

Baron, Chris and Bob Weil, "Implementing a Web Shopping Cart," *Dr. Dobb's Journal*, Sep. 1996, pp. 64, 66, 68–69, and 83–85.

Hoque, Reaz, "A Shopping Cart Application with JavaScript," *Web Techniques*, May 1998, pp. 63, 65–66, and 68.

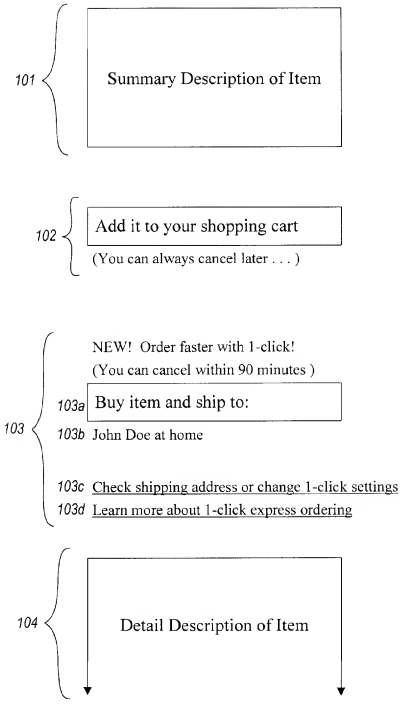

101
Summary Description of Item
102
Add it to your shopping cart
(You can always cancel later . . .)
103
NEW! Order faster with 1-click!
(You can cancel within 90 minutes)
103a Buy item and ship to:
103b John Doe at home
103c Check shipping address or change 1-click settings
103d Learn more about 1-click express ordering
104
Detail Description of Item

Fig. 1A

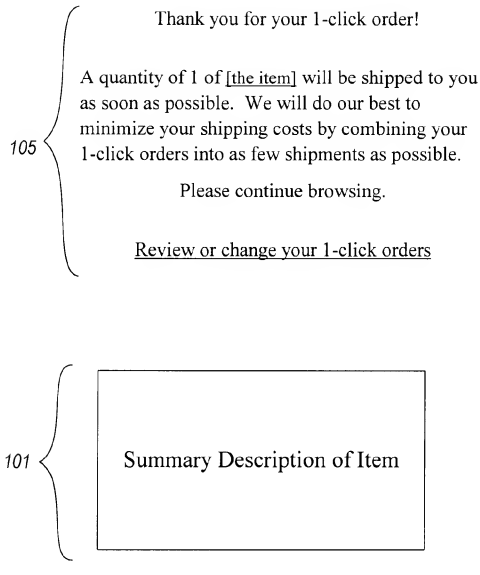

Thank you for your 1-click order!
A quantity of 1 of [the item] will be shipped to you as soon as possible. We will do our best to minimize your shipping costs by combining your 1-click orders into as few shipments as possible.
105
Please continue browsing.
Review or change your 1-click orders
101
Summary Description of Item

Fig. 1B

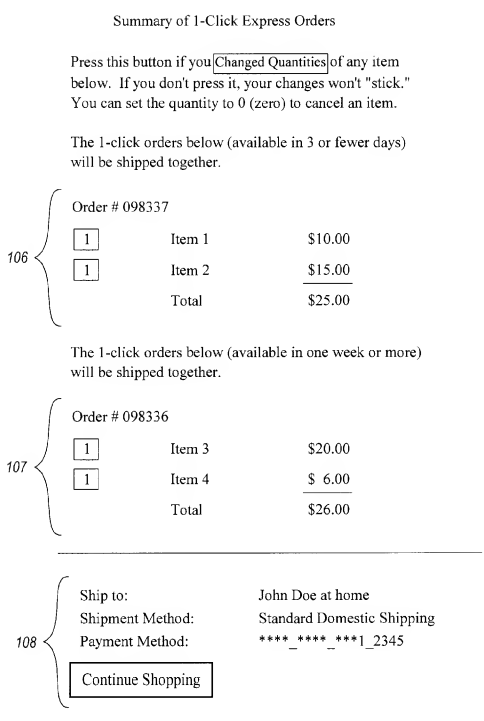

Summary of 1-Click Express Orders
Press this button if you Changed Quantities of any item below. If you don't press it, your changes won't "stick." You can set the quantity to 0 (zero) to cancel an item.
The 1-click orders below (available in 3 or fewer days) will be shipped together.
106
Order # 098337
1 Item 1 $10.00
1 Item 2 $15.00
Total $25.00
The 1-click orders below (available in one week or more) will be shipped together.
107
Order # 098336
1 Item 3 $20.00
1 Item 4 $ 6.00
Total $26.00
108
Ship to: John Doe at home
Shipment Method: Standard Domestic Shipping
Payment Method: ****_****_***1_2345
Continue Shopping
1-Click Express shipping policies

Fig. 1C

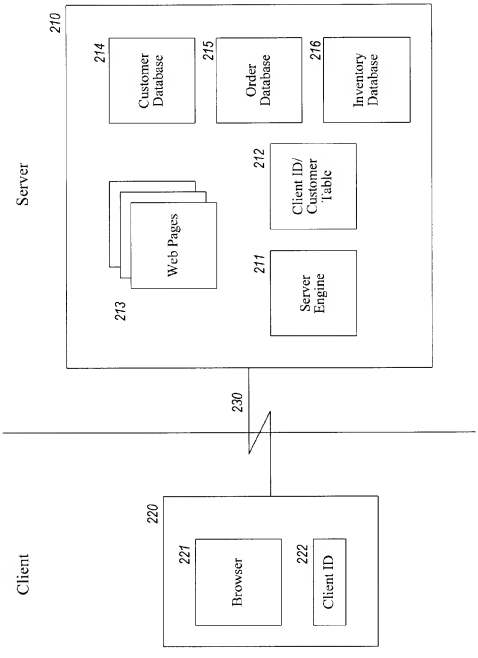

Client
Server
210
214
Customer Database
215
Order Database
216
Inventory Database
212
Client ID/ Customer Table
213
Web Pages
211
Server Engine
230
220
221
Browser
222
Client ID

Fig. 2

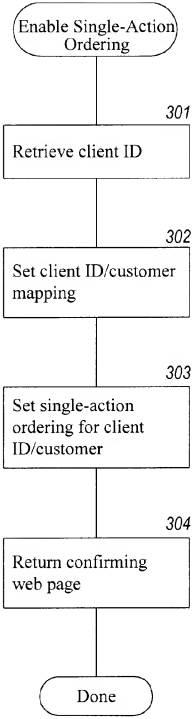

Enable Single-Action Ordering
301
Retrieve client ID
302
Set client ID/customer mapping
303
Set single-action ordering for client ID/customer
304
Return confirming web page
Done

Fig. 3

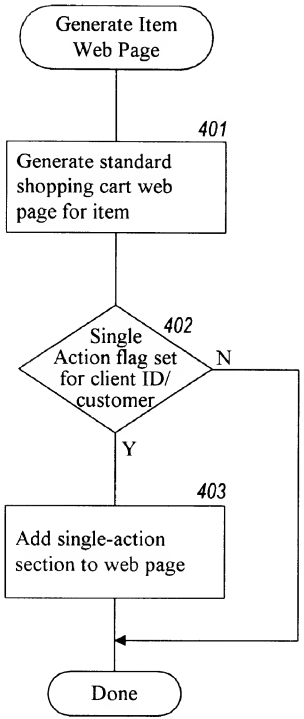

Generate Item Web Page
401
Generate standard shopping cart web page for item
402
Single Action flag set for client ID/ customer
N
Y
403
Add single-action section to web page
Done

Fig. 4

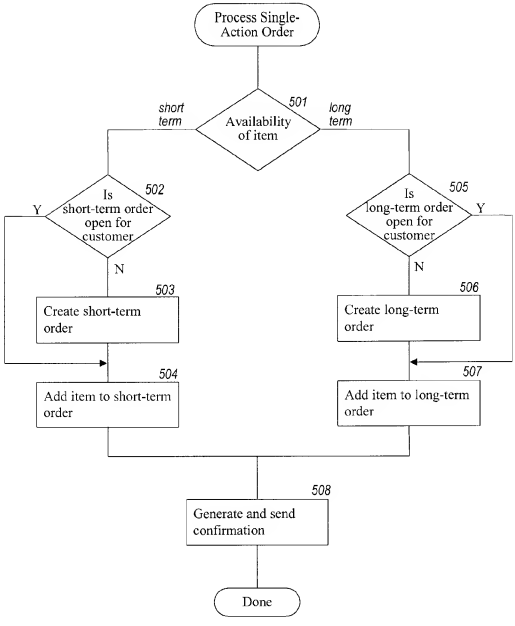

Process Single-Action Order
501
Availability of item
short term
long term
502
Is short-term order open for customer
Y
N
503
Create short-term order
504
Add item to short-term order
505
Is long-term order open for customer
Y
N
506
Create long-term order
507
Add item to long-term order
508
Generate and send confirmation
Done

Fig. 5

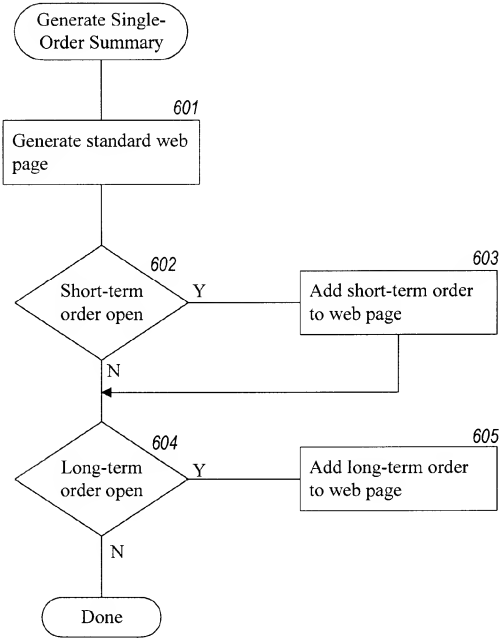

Generate Single-Order Summary
601
Generate standard web page
602
Short-term order open
Y
603
Add short-term order to web page
N
604
Long-term order open
Y
605
Add long-term order to web page
N
Done

Fig. 6

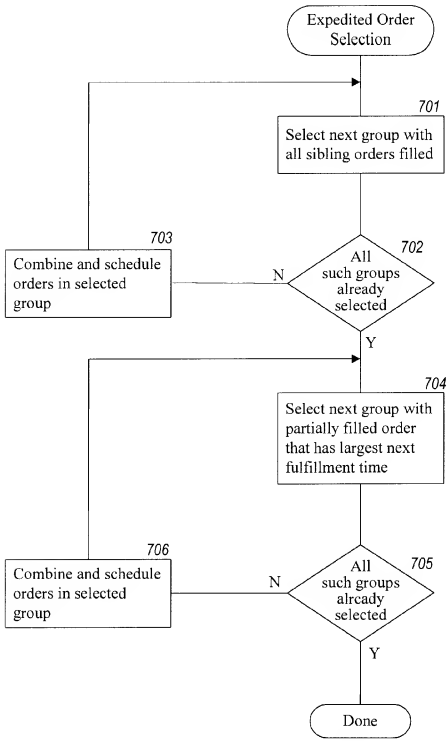

Expedited Order Selection
701
Select next group with all sibling orders filled
702
All such groups already selected
N
703
Combine and schedule orders in selected group
Y
704
Select next group with partially filled order that has largest next fulfillment time
705
All such groups already selected
N
706
Combine and schedule orders in selected group
Y
Done

Fig. 7


START
A: Customer Name & Address
B: Customer Financial Info
C: Customer Employment Info
D: Customer Education Info

Fig. 8A

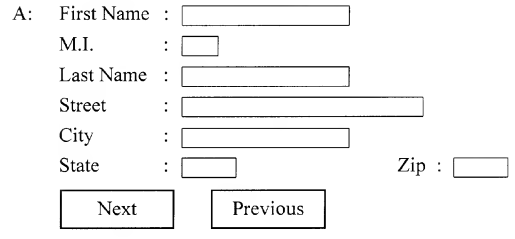

A: First Name :
M.I. :
Last Name :
Street :
City :
State :
Zip :
Next
Previous
B: Customer Financial Info
C: Customer Employment Info
D: Customer Education Info

Fig. 8B

A: Customer Name & Address

B: Net Worth: [ ]

Annual Income: [ ]

Spouse's Annual Income: [ ]

Other Income: [ ]

[Next] [Previous]

C: Customer Employment Info

D: Customer Education Info

.
.
.

Fig. 8C

METHOD AND SYSTEM FOR PLACING A PURCHASE ORDER VIA A COMMUNICATIONS NETWORK

TECHNICAL FIELD

The present invention relates to a computer method and system for placing an order and, more particularly, to a method and system for ordering items over the Internet.

BACKGROUND OF THE INVENTION

The Internet comprises a vast number of computers and computer networks that are interconnected through communication links. The interconnected computers exchange information using various services, such as electronic mail, Gopher, and the World Wide Web ("WWW"). The WWW service allows a server computer system (i.e., Web server or Web site) to send graphical Web pages of information to a remote client computer system. The remote client computer system can then display the Web pages. Each resource (e.g., computer or Web page) of the WWW is uniquely identifiable by a Uniform Resource Locator ("URL"). To view a specific Web page, a client computer system specifies the URL for that Web page in a request (e.g., a HyperText Transfer Protocol ("HTTP") request). The request is forwarded to the Web server that supports that Web page. When that Web server receives the request, it sends that Web page to the client computer system. When the client computer system receives that Web page, it typically displays the Web page using a browser. A browser is a special-purpose application program that effects the requesting of Web pages and the displaying of Web pages.

Currently, Web pages are typically defined using HyperText Markup Language ("HTML"). HTML provides a standard set of tags that define how a Web page is to be displayed. When a user indicates to the browser to display a Web page, the browser sends a request to the server computer system to transfer to the client computer system an HTML document that defines the Web page. When the requested HTML document is received by the client computer system, the browser displays the Web page as defined by the HTML document. The HTML document contains various tags that control the displaying of text, graphics, controls, and other features. The HTML document may contain URLs of other Web pages available on that server computer system or other server computer systems.

The World Wide Web is especially conducive to conducting electronic commerce. Many Web servers have been developed through which vendors can advertise and sell product. The products can include items (e.g., music) that are delivered electronically to the purchaser over the Internet and items (e.g., books) that are delivered through conventional distribution channels (e.g., a common carrier). A server computer system may provide an electronic version of a catalog that lists the items that are available. A user, who is a potential purchaser, may browse through the catalog using a browser and select various items that are to be purchased. When the user has completed selecting the items to be purchased, the server computer system then prompts the user for information to complete the ordering of the items. This purchaser-specific order information may include the purchaser's name, the purchaser's credit card number, and a shipping address for the order. The server computer system then typically confirms the order by sending a confirming Web page to the client computer system and schedules shipment of the items.

Since the purchaser-specific order information contains sensitive information (e.g., a credit card number), both

vendors and purchasers want to ensure the security of such information. Security is a concern because information transmitted over the Internet may pass through various intermediate computer systems on its way to its final destination. The information could be intercepted by an unscrupulous person at an intermediate system. To help ensure the security of the sensitive information, various encryption techniques are used when transmitting such information between a client computer system and a server computer system. Even though such encrypted information can be intercepted, because the information is encrypted, it is generally useless to the interceptor. Nevertheless, there is always a possibility that such sensitive information may be successfully decrypted by the interceptor. Therefore, it would be desirable to minimize the sensitive information transmitted when placing an order.

The selection of the various items from the electronic catalogs is generally based on the "shopping cart" model. When the purchaser selects an item from the electronic catalog, the server computer system metaphorically adds that item to a shopping cart. When the purchaser is done selecting items, then all the items in the shopping cart are "checked out" (i.e., ordered) when the purchaser provides billing and shipment information. In some models, when a purchaser selects any one item, then that item is "checked out" by automatically prompting the user for the billing and shipment information. Although the shopping cart model is very flexible and intuitive, it has a downside in that it requires many interactions by the purchaser. For example, the purchaser selects the various items from the electronic catalog, and then indicates that the selection is complete. The purchaser is then presented with an order Web page that prompts the purchaser for the purchaser-specific order information to complete the order. That Web page may be prefilled with information that was provided by the purchaser when placing another order. The information is then validated by the server computer system, and the order is completed. Such an ordering model can be problematic for a couple of reasons. If a purchaser is ordering only one item, then the overhead of confirming the various steps of the ordering process and waiting for, viewing, and updating the purchaser-specific order information can be much more than the overhead of selecting the item itself. This overhead makes the purchase of a single item cumbersome. Also, with such an ordering model, each time an order is placed sensitive information is transmitted over the Internet. Each time the sensitive information is transmitted over the Internet, it is susceptible to being intercepted and decrypted.

SUMMARY OF THE INVENTION

An embodiment of the present invention provides a method and system for ordering an item from a client system. The client system is provided with an identifier that identifies a customer. The client system displays information that identifies the item and displays an indication of an action (e.g., a single action such as clicking a mouse button) that a purchaser is to perform to order the identified item. In response to the indicated action being performed, the client system sends to a server system the provided identifier and a request to order the identified item. The server system uses the identifier to identify additional information needed to generate an order for the item and then generates the order.

The server system receives and stores the additional information for customers using various computer systems so that the server system can generate such orders. The server system stores the received additional information in association with an identifier of the customer and provides

the identifier to the client system. When requested by the client system, the server system provides information describing the item to the requesting client system. When the server system receives a request from a client system, the server system combines the additional information stored in association with the identifier included in the request to effect the ordering of the item.

BRIEF DESCRIPTION OF THE DRAWINGS

FIGS. **1A–1C** illustrate single-action ordering in one embodiment of the present invention.

FIG. **2** is a block diagram illustrating an embodiment of the present invention.

FIG. **3** is a flow diagram of a routine that enables single-action ordering for a customer.

FIG. **4** is a flow diagram of a routine to generate a Web page in which single-action ordering is enabled.

FIG. **5** is a flow diagram of a routine which processes a single-action order.

FIG. **6** is a flow diagram of a routine for generating a single-action order summary Web page.

FIG. **7** is a flow diagram of a routine that implements an expedited order selection algorithm.

FIGS. **8A–8C** illustrate a hierarchical data entry mechanism in one embodiment.

DETAILED DESCRIPTION OF THE INVENTION

The present invention provides a method and system for single-action ordering of items in a client/server environment. The single-action ordering system of the present invention reduces the number of purchaser interactions needed to place an order and reduces the amount of sensitive information that is transmitted between a client system and a server system. In one embodiment, the server system assigns a unique client identifier to each client system. The server system also stores purchaser-specific order information for various potential purchasers. The purchaser-specific order information may have been collected from a previous order placed by the purchaser. The server system maps each client identifier to a purchaser that may use that client system to place an order. The server system may map the client identifiers to the purchaser who last placed an order using that client system. When a purchaser wants to place an order, the purchaser uses a client system to send the request for information describing the item to be ordered along with its client identifier. The server system determines whether the client identifier for that client system is mapped to a purchaser. If so mapped, the server system determines whether single-action ordering is enabled for that purchaser at that client system. If enabled, the server system sends the requested information (e.g., via a Web page) to the client computer system along with an indication of the single action to perform to place the order for the item. When single-action ordering is enabled, the purchaser need only perform a single action (e.g., click a mouse button) to order the item. When the purchaser performs that single action, the client system notifies the server system. The server system then completes the order by adding the purchaser-specific order information for the purchaser that is mapped to that client identifier to the item order information (e.g., product identifier and quantity). Thus, once the description of an item is displayed, the purchaser need only take a single action to place the order to purchase that item. Also, since the client identifier identifies purchaser-specific order information already stored at the server system, there is no need for such sensitive information to be transmitted via the Internet or other communications medium.

FIGS. **1A–1C** illustrate single-action ordering in one embodiment of the present invention. FIG. **1A** illustrates the display of a Web page describing an item that may be ordered. This example Web page was sent from the server system to the client system when the purchaser requested to review detailed information about the item. This example Web page contains a summary description section **101**, a shopping cart section **102**, a single-action ordering section **103**, and a detailed description section **104**. One skilled in the art would appreciate that these various sections can be omitted or rearranged or adapted in various ways. In general, the purchaser need only be aware of the item or items to be ordered by the single action and of the single action needed to place the order. The summary description and the detailed description sections provide information that identifies and describes the item(s) that may be ordered. The shopping cart section provides the conventional capability to add the described item to a shopping cart. The server system adds the summary description, the detailed description, and the shopping cart sections to each Web page for an item that may be ordered. The server system, however, only adds the single-action ordering section when single-action ordering is enabled for that purchaser at that client system. (One skilled in the art would appreciate that a single Web page on the server system may contain all these sections but the single-action ordering section can be selectively included or excluded before sending the Web page to the client system.) This example single-action ordering section allows the purchaser to specify with a single click of a mouse button to order the described item. Once the purchaser clicks the mouse button, the item is ordered, unless the purchaser then takes some action to modify the order. The single-action ordering section contains a single-action ordering button **103***a*, purchaser identification subsection **103***b*, and single-action ordering information subsections **103***c* and **103***d*. The purchaser information subsection displays enough information so that the purchaser can verify that the server system correctly recognizes the purchaser. To reduce the chances of sensitive information being intercepted, the server system sends only enough information so that the purchaser is confident that the server system correctly identified the purchaser but yet not enough information to be useful to an unscrupulous interceptor. The additional information subsections allow the purchaser to obtain various settings or obtain more information related to the single-action ordering. If the purchaser wants to verify the shipping address, the purchaser can select the "check shipping address" label. In response to this selection, the server system may require the purchaser to perform a "login" so that the identity of the purchaser can be verified before the shipping information is viewed or modified. The server system then sends a Web page to the client system for display and possible modification of the shipping address. In this way, the transmitting of the sensitive shipping address can be avoided unless requested by the verified purchaser.

When the purchaser selects the single-action ordering button, the client system sends a message to the server system requesting that the displayed item be ordered. After the server system processes the message, the server system provides to the client system a new Web page that confirms receipt of the single-action order. FIG. **1B** illustrates the display of a Web page confirming a single-action order. The confirming Web page contains essentially the same information as the Web page describing the item (i.e., FIG. **1A**)

except that an order confirmation section **105** is displayed at the top of the Web page. The order confirmation section confirms that the order has been placed and provides an opportunity for the purchaser to review and change the single-action order. Alternatively, the confirming Web page can be identical to the Web page describing the item (i.e., FIG. 1A), except that the single-action ordering button is replaced with a message confirming the order.

If a single-action ordering is not currently enabled for the client system but could be enabled, then the server system can generate a Web page like FIG. 1A, except that the single-action ordering button **103***a* is replaced by a single-action ordering enable button. Such a replacement button could contain text instructing the purchaser to click on the button to enable single-action ordering. When the purchaser clicks on that button, the server system would send the Web page of FIG. 1A to be displayed. Single-action ordering can be enabled whenever the server system has stored sufficient purchaser-specific order information for that client system to complete a single-action order. If the server system does not have sufficient information, then when the purchaser selects the single-action ordering button, the server system can provide a Web page to collect the additional information that is needed. The server system may require the purchaser to "login" so that the identity of the purchaser can be verified before the single-action ordering is enabled.

To help minimize shipping costs and purchaser confusion, the server system may combine various single-action orders into a multiple-item order. For example, if a purchaser orders one item using the single-action ordering and five minutes later orders another item using the single-action ordering, then those orders may be cost effectively combined into a single order for shipping. The server system combines the single-action orders when their expected ship dates are similar. For example, if one item is immediately available and the other item will be available in one day, then the two single-action orders may be cost-effectively combined. However, if the other item will not be available for two weeks, then the two single-item orders would not be combined. FIG. 1C illustrates the display of a Web page representing four single-action orders that have been combined into two separate multiple-item orders based on the availability of the items. The order information **106** indicates that item 1 and item **2**, which will be available in three or fewer days, have been combined into one order. The order information **107** indicates that items **3** and **4**, which will not be available within one week, are combined into a separate order. In one embodiment, the server system may combine single-action orders that are placed within a certain time period (e.g., 90 minutes). Also, the server system may combine or divide orders when the orders are scheduled for shipment based on the then current availability of the items ordered. This delayed modification of the orders is referred to as "expedited order selection" and is described below in detail.

FIG. **2** is a block diagram illustrating an embodiment of the present invention. This embodiment supports the single-action ordering over the Internet using the World Wide Web. The server system **210** includes a server engine **211**, a client identifier/customer table **212**, various Web pages **213**, a customer database **214**, an order database **215**, and an inventory database **216**. The server engine receives HTTP requests to access Web pages identified by URLs and provides the Web pages to the various client systems. Such an HTTP request may indicate that the purchaser has performed the single action to effect single-action ordering. The customer database contains customer information for various purchasers or potential purchasers. The customer information includes purchaser-specific order information such as the name of the customer, billing information, and shipping information. The order database **215** contains an entry for each order that has not yet been shipped to a purchaser. The inventory database **216** contains a description of the various items that may be ordered. The client identifier/customer table **212** contains a mapping from each client identifier, which is a globally unique identifier that uniquely identifies a client system, to the customer last associated with that client system. The client system **220** contains a browser and its assigned client identifier. The client identifier is stored in a file, referred to as a "cookie." In one embodiment, the server system assigns and sends the client identifier to the client system once when the client system first interacts with the server system. From then on, the client system includes its client identifier with all messages sent to the server system so that the server system can identify the source of the message. The server and client systems interact by exchanging information via communications link **230**, which may include transmission over the Internet.

One skilled in the art would appreciate that the single-action ordering techniques can be used in various environments other than the Internet. For example, single-action ordering can also be in an electronic mail environment in which an item is described in an electronic mail message along with an indication of the single action that is to be performed to effect the ordering of the item. Also, various communication channels may be used such as local area network, wide area network, or point-to-point dial up connection. Also, a server system may comprise any combination of hardware or software that can generate orders in response to the single action being performed. A client system may comprise any combination of hardware or software that can interact with the server system. These systems may include television-based systems or various other consumer products through which orders may be placed.

FIG. **3** is a flow diagram of a routine that enables single-action ordering for a customer. To enable single-action ordering, a server system needs to have information about the customer that is equivalent to the purchaser-specific order information. The server system can obtain this information in various ways. First, the server system could ask the customer if they would like to have single-action ordering enabled. If so, then the server system could prompt the customer using a Web page for the purchaser-specific order information. Second, the server system could also save the purchaser-specific order information collected when an order is placed conventionally. The server system could, either automatically or with the customer's assent, enable single-action ordering. In step **301**, the server system retrieves the client identifier that was sent by the client system. In step **302**, the server system updates the client identifier/customer table to indicate that the generated client identifier has been associated with that customer. In step **303**, the server system sets a flag indicating that single-action ordering is enabled for that client identifier and that customer combination. That flag may be stored in the client identifier/customer table. In step **304**, the server system supplies a confirming Web page to the client system. The next time a purchaser attempts to order an item, the client system will supply its client identifier to the server system. If single-action ordering is enabled for that purchaser, the server system will assume that the purchaser is the customer associated with that client identifier in the client identifier/customer table. Thus, a purchaser may not want to allow the

server system to enable single-action ordering if there is a possibility that someone else may use that same client system.

FIG. **4** is a flow diagram of a routine to generate a Web page in which single-action ordering is enabled. When single-action ordering is enabled, the server system generates a Web page describing an item as is conventionally done and then adds a single-action ordering section. In one embodiment, the server system adds partial purchaser-specific order information to the section. This information may include the customer's name, a shipping address moniker selected by the purchaser (e.g., "at home"), and the last five digits of a credit card number or a nickname selected by the purchaser. Such partial information should be the minimum information sufficient to indicate to the purchaser whether or not the server system is using the correct purchaser-specific order information. In step **401**, the server system generates a standard shopping cart-type Web page for the item. In step **402**, if the single-action ordering flag has been set for the client identifier and customer combination, then the server system continues at step **403**, else the server system completes. In step **403**, the server system adds the single-action section to the Web page and completes.

FIG. **5** is a flow diagram of a routine which processes a single-action order. When a purchaser performs the single action needed to place an order, the client system notifies the server system. The server system then combines the purchaser-specific order information for the customer associated with the client system with the item order information to complete the order. The single-action order may also be combined with other single-action orders and possibly with other conventionally placed orders to reduce shipping costs. In one embodiment, single-action orders can be combined if they are placed within a certain time period of each other (e.g., 90 minutes). This routine illustrates the combining of the single-action orders into a short-term order (e.g., available to be shipped in less than a week) and a long-term order (e.g., available to be shipped in more than a week). One skilled in the art would appreciate that the single-action orders can be combined in various ways based on other factors, such as size of shipment and intermediate-term availability. In step **501**, if the item is expected to be shipped in the short term, then the server system continues at step **502**, else the server system continues at step **505**. In step **502**, if a short-term order has already been opened for the purchaser, then the server system continues at step **504**, else the server system continues at step **503**. In step **503**, the server system creates a short-term order for the purchaser. In step **504**, the server system adds the item to the short-term order and continues at step **508**. In step **505**, if a long-term order has already been opened for the purchaser, then the server system continues at step **507**, else the server system continues at step **506**. In step **506**, the server system creates a long-term order for the purchaser. In step **507**, the server system adds the item to the long-term order. In step **508**, the server system generates and sends the confirmation and completes.

FIG. **6** is a flow diagram of a routine for generating a single-action order summary Web page. This Web page (e.g., FIG. 1C) gives the user the opportunity to view and modify the short-term and long-term single-action orders. In step **601**, the server system adds the standard single-action order information to the Web page. In step **602**, if a short-term order is open, then the server system adds the short-term order to the Web page in step **603**. In step **604**, if a long-term order is open, then the server system adds the long-term order information to the Web page in step **605** and completes.

FIG. **7** is a flow diagram of a routine that implements an expedited order selection algorithm. The goal of the expedited order selection algorithm is to minimize the number of orders sent to each destination so that shipping costs are reduced. A destination may be a specific shipping address plus a specific purchaser's billing details. Orders that are sent to the same destination are known as "sibling orders." The algorithm has two stages. In the first stage, the algorithm schedules for shipment the orders for destinations for which all the sibling orders are filled. An order is filled when all its items are currently in inventory (i.e., available) and can be shipped. For each group of sibling orders, the algorithm combines those sibling orders into a single combined order so that only one order is currently scheduled for shipment to each destination. In the second stage, the algorithm combines and schedules groups of sibling orders for which some of the sibling orders are not filled or partially filled. The algorithm may split each partially filled sibling order into a filled sibling order and a completely unfilled sibling order. The algorithm then combines all the filled sibling orders into a single combined order and schedules the combined order for shipment. If any group has only one sibling order and that order is partially filled, then the algorithm in one embodiment does not split that order to avoid making an extra shipment to that destination.

During the second stage, the algorithm may select and schedule groups of sibling orders in a sequence that is based on the next fulfillment time for an item in the group. The next fulfillment time for a group of sibling orders is the minimum expected fulfillment time of the items in that group of sibling orders. For example, if a group of sibling orders has seven items that are not yet fulfilled and their expected fulfillment times range from 3 days to 14 days, then the next fulfillment time for that group is 3 days. The algorithm first schedules those groups of sibling orders with the largest next fulfillment time. For example, if 6 groups have next fulfillment times of 3, 5, 7, 10, 11, and 14 days, respectively, then the algorithm first selects and schedules the sibling orders in the group with the next fulfillment time of 14 days, followed by the group with the next fulfillment time of 11 days, and so on. By delaying the scheduling of groups with short next fulfillment times, the algorithm increases the chances of additional items becoming available (because of the shortness of the next fulfillment time) and thus combined with the scheduled order.

Steps **701**–**703** represent the first stage of the expedited order selection algorithm, and steps **704**–**706** represent the second stage of the expedited selection order algorithm. In steps **701**–**703**, the algorithm loops selecting groups in which all sibling orders are filled and combining the orders. In step **701**, the algorithm selects the next group with all sibling orders that are filled. In step **703**, if all such groups have already been selected, then the algorithm continues with the second stage in step **704**, else the algorithm continues at step **703**. In step **703**, the algorithm combines and schedules the orders in the selected group and loops to step **701**. In step **704**, the algorithm selects the next group of sibling orders that has the largest next fulfillment time. In step **705**, if all such groups have already been selected, then the algorithm is done, else the algorithm continues at step **706**. In step **706**, the algorithm combines and schedules the orders in the selected group and loops to step **704**. When the expedited order selection algorithm is being performed, new orders and new inventory may be received. Whenever such new orders and new inventory is received, then the algorithm restarts to schedule and combine the new orders as appropriate.

Although the algorithm has been described as having two stages, it could be implemented in an incremental fashion where the assessment of the first and second stages are redone after each order is scheduled. One skilled in the art would recognize that there are other possible combinations of these stages which still express the same essential algorithm.

FIGS. **8**A–**8**C illustrate a hierarchical data entry mechanism in one embodiment. When collecting information from a user, a Web page typically consists of a long series of data entry fields that may not all fit onto the display at the same time. Thus, a user needs to scroll through the Web page to enter the information. When the data entry fields do not fit onto the display at the same time, it is difficult for the user to get an overall understanding of the type and organization of the data to be entered. The hierarchical data entry mechanism allows a user to understand the overall organization of the data to be entered even though the all data entry fields would not fit onto the display at the same time. FIG. **8**A illustrates an outline format of a sample form to be filled in. The sample form contains various sections identified by letters A, B, C, and D. When the user selects the start button, then section A expands to include the data entry fields for the customer name and address. FIG. **8**B illustrates the expansion of section A. Since only section A has been expanded, the user can view the data entry fields of section A and summary information of the other sections at the same time. The user then enters data in the various data entry fields that are displayed. Upon completion, the user selects either the next or previous buttons. The next button causes section A to be collapsed and section B to be expanded so that financial information may be entered. FIG. **8**C illustrates the expansion of section B. If the previous button is selected, then section A would collapse and be displayed as shown in FIG. **8**A. This collapsing and expanding is repeated for each section. At any time during the data entry, if an error is detected, then a Web page is generated with the error message in close proximity (e.g., on the line below) to the data entry field that contains the error. This Web page is then displayed by the client system to inform the user of the error. In addition, each of the data "entry" fields may not be editable until the user clicks on the data entry field or selects an edit button associated with the data entry field. In this way, the user is prevented from inadvertently changing the contents of an edit field. When the user clicks on a data entry field, a new Web page is presented to the user that allows for the editing of the data associated with the field. When editing is complete, the edited data is displayed in the data "entry" field Because the fields of the form are thus not directly editable, neither "named-submit" buttons nor Java are needed. Also, the form is more compact because the various data entry options (e.g., radio button) are displayed only on the new Web page when the field is to be edited.

Although the present invention has been described in terms of various embodiments, it is not intended that the invention be limited to these embodiments. Modification within the spirit of the invention will be apparent to those skilled in the art. For example, the server system can map a client identifier to multiple customers who have recently used the client system. The server system can then allow the user to identify themselves by selecting one of the mappings based preferably on a display of partial purchaser-specific order information. Also, various different single actions can be used to effect the placement of an order. For example, a voice command may be spoken by the purchaser, a key may be depressed by the purchaser, a button on a television remote control device may be depressed by the purchaser, or selection using any pointing device may be effected by the purchaser. Although a single action may be preceded by multiple physical movements of the purchaser (e.g., moving a mouse so that a mouse pointer is over a button), the single action generally refers to a single event received by a client system that indicates to place the order. Finally, the purchaser can be alternately identified by a unique customer identifier that is provided by the customer when the customer initiates access to the server system and sent to the server system with each message. This customer identifier could be also stored persistently on the client system so that the purchaser does not need to re-enter their customer identifier each time access is initiated. The scope of the present invention is defined by the claims that follow.

We claim:

1. A method of placing an order for an item comprising:

under control of a client system,

displaying information identifying the item; and

in response to only a single action being performed, sending a request to order the item along with an identifier of a purchaser of the item to a server system;

under control of a single-action ordering component of the server system,

receiving the request;

retrieving additional information previously stored for the purchaser identified by the identifier in the received request; and

generating an order to purchase the requested item for the purchaser identified by the identifier in the received request using the retrieved additional information; and

fulfilling the generated order to complete purchase of the item

whereby the item is ordered without using a shopping cart ordering model.

2. The method of claim **1** wherein the displaying of information includes displaying information indicating the single action.

3. The method of claim **1** wherein the single action is clicking a button.

4. The method of claim **1** wherein the single action is speaking of a sound.

5. The method of claim **1** wherein a user of the client system does not need to explicitly identify themselves when placing an order.

6. A client system for ordering an item comprising:

an identifier that identifies a customer;

a display component for displaying information identifying the item;

a single-action ordering component that in response to performance of only a single action, sends a request to a server system to order the identified item, the request including the identifier so that the server system can locate additional information needed to complete the order and so that the server system can fulfill the generated order to complete purchase of the item; and

a shopping cart ordering component that in response to performance of an add-to-shopping-cart action, sends a request to the server system to add the item to a shopping cart.

7. The client system of claim **6** wherein the display component is a browser.

8. The client system of claim **6** wherein the predefined action is the clicking of a mouse button

9. A server system for generating an order comprising:

a shopping cart ordering component; and

a single-action ordering component including:

a data storage medium storing information for a plurality of users;

a receiving component for receiving requests to order an item, a request including an indication of one of the plurality of users, the request being sent in response to only a single action being performed; and

an order placement component that retrieves from the data storage medium information for the indicated user and that uses the retrieved information to place an order for the indicated user for the item; and

an order fulfillment component that completes a purchase of the item in accordance with the order placed by the single-action ordering component.

10. The server system of claim **9** wherein the request is sent by a client system in response to a single action being performed.

11. A method for ordering an item using a client system, the method comprising:

displaying information identifying the item and displaying an indication of a single action that is to be performed to order the identified item; and

in response to only the indicated single action being performed, sending to a server system a request to order the identified item

whereby the item is ordered independently of a shopping cart model and the order is fulfilled to complete a purchase of the item.

12. The method of claim **11** wherein the server system uses an identifier sent along with the request to identify additional information needed to generate an order for the item.

13. The method of claim **12** wherein the identifier identifies the client system and the server system provides the identifier to the client system.

14. The method of claim **11** wherein the client system and server system communicate via the Internet.

15. The method of claim **11** wherein the displaying includes displaying an HTML document provided by the server system.

16. The method of claim **11** including sending from the server system to the client system a confirmation that the order was generated.

17. The method of claim **11** wherein the single action is clicking a mouse button when a cursor is positioned over a predefined area of the displayed information.

18. The method of claim **11** wherein the single action is a sound generated by a user.

19. The method of claim **11** wherein the single action is selection using a television remote control.

20. The method of claim **11** wherein the single action is depressing of a key on a key pad.

21. The method of claim **11** wherein the single action is selecting using a pointing device.

22. The method of claim **11** wherein the single action is selection of a displayed indication.

23. The method of claim **11** wherein the displaying includes displaying partial information supplied by the server system as to the identity of a user of the client system.

24. The method of claim **11** wherein the displaying includes displaying partial shipping information supplied by the server system.

25. The method of claim **11** wherein the displaying includes displaying partial payment information supplied by the server system.

26. The method of claim **11** wherein the displaying includes displaying a moniker identifying a shipping address for the customer.

* * * * *

US006311214B1

(12) **United States Patent**
Rhoads

(10) **Patent No.: US 6,311,214 B1**
(45) **Date of Patent: *Oct. 30, 2001**

(54) **LINKING OF COMPUTERS BASED ON OPTICAL SENSING OF DIGITAL DATA**

(75) Inventor: **Geoffrey B. Rhoads**, West Linn, OR (US)

(73) Assignee: **Digimarc Corporation**, Tualatin, OR (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **09/342,689**

(22) Filed: **Jun. 29, 1999**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/130,624, filed on Aug. 6, 1998, which is a continuation of application No. 08/508,083, filed on Jul. 27, 1995, now Pat. No. 5,841,978, and a continuation-in-part of application No. 09/314,648, filed on May 19, 1999, which is a continuation-in-part of application No. 09/292,569, filed on Apr. 15, 1999.
(60) Provisional application No. 60/134,782, filed on May 19, 1999.

(51) **Int. Cl.**[7] **G06F 13/00**
(52) **U.S. Cl.** **709/217**; 709/313; 380/4
(58) **Field of Search** 709/217, 219, 709/227, 230, 250, 313, 328, 329; 380/4, 9, 49

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,947,028 8/1990 Gorog .
5,053,956 10/1991 Donald et al. .
5,262,860 11/1993 Fitzpatrick et al. .
5,288,976 2/1994 Citron et al. .
5,385,371 1/1995 Izawa .
5,463,209 10/1995 Figh et al. .
5,495,581 2/1996 Tsai .

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0493091 7/1992 (EP) .
WO95/14289 5/1995 (WO) .
WO95/20291 7/1995 (WO) .
WO96/27259 9/1996 (WO) .
WO96/36163 11/1996 (WO) .
WO97/02522 1/1997 (WO) .
WO97/43736 11/1997 (WO) .
WO98/03923 1/1998 (WO) .
WO98/51036 11/1998 (WO) .
WO99/57623 11/1999 (WO) .

OTHER PUBLICATIONS

U.S. application No. 60/000,442, Hudetz, filed Jun. 22, 1995.

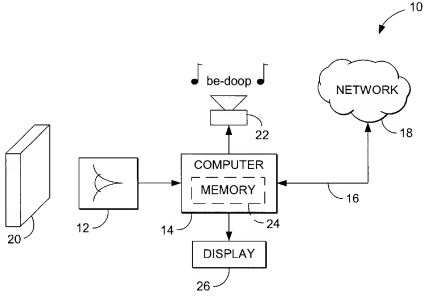
(List continued on next page.)

Primary Examiner—Viet D. Vu
(74) *Attorney, Agent, or Firm*—William Y. Conwell; Digimarc Corporation

(57) **ABSTRACT**

A printed object, such as an item of postal mail, a book, printed advertising, a business card, product packaging, etc., is steganographically encoded with plural-bit data. When such an object is presented to an optical sensor, the plural-bit data is decoded and used to establish a link to an internet address corresponding to that object.

23 Claims, 2 Drawing Sheets



U.S. PATENT DOCUMENTS

5,496,071		3/1996	Walsh .
5,530,852		6/1996	Meske, Jr. et al. .
5,613,004		3/1997	Cooperman et al. .
5,640,193		6/1997	Wellner .
5,659,164		8/1997	Schmid et al. .
5,673,316		9/1997	Auerbach et al. .
5,721,788		2/1998	Powell et al. .
5,742,845		4/1998	Wagner .
5,761,606		6/1998	Wolzien .
5,761,686		6/1998	Bloomberg .
5,774,664		6/1998	Hidary et al. .
5,774,666		6/1998	Portuesi .
5,778,102		7/1998	Sandford, II et al. .
5,804,803		9/1998	Cragun et al. .
5,809,317		9/1998	Kogan et al. .
5,818,441		10/1998	Throckmorton et al. .
5,822,432		10/1998	Moskowitz et al. .
5,838,458		11/1998	Tsai .
5,848,413	*	12/1998	Wolff 707/10
5,857,038		1/1999	Owada et al. .
5,872,589		2/1999	Morales .
5,892,900		4/1999	Ginter et al. .
5,900,608		5/1999	Iida .
5,903,729		5/1999	Reber et al. .
5,905,248	*	5/1999	Russell et al. 235/462.27
5,913,210		6/1999	Call .
5,915,027		6/1999	Cox et al. .
5,918,214		6/1999	Perkowski .
5,932,863		8/1999	Rathus et al. .
5,933,829		8/1999	Durst et al. .
5,938,726		8/1999	Reber et al. .
5,940,595		8/1999	Reber et al. .
5,978,773		11/1999	Hudetz et al. .
5,986,651		11/1999	Reber et al. .
6,012,102		1/2000	Shachar .
6,052,486		4/2000	Knowlton et al. .
6,081,827		6/2000	Reber et al. .
6,098,106		8/2000	Philyaw et al. .
6,108,656		8/2000	Durst et al. .
6,148,331		11/2000	Parry .

OTHER PUBLICATIONS

IBM Technical Disclosure Bulletin 96A 61092, published Jan. 1, 1996.

"Distributing Uniform Resource Locators as Bar Code Images," IBM Technical Disclosure Bulletin, No. 39, No. 1, pp. 167–168, 96A 60059, published Jan. 1, 1996.

Frequently Asked Questions about Digimarc Signature Technology, Aug. 1, 1995, 9 pages.

Bartlett, et al., "An Overview of HighWater FBI Technology," Posted on Internet Mar. 22, 1996, 12 pages.

Digimarc presentation at RSA Conference, Jan. 1996, 4 pages.

"Digital Watermarks What Are They?" Digimarc Corporation, 1997.

Seybold Report on Internet Publishing, vol. 1, No. 4, Dec. 1996.

Seybold Report on Publishing Systems, vol. 25, No. 6, 1996.

Bethoney, "A Lasting Way For Artists To Leave Their Mark," PCWeek, Dec. 11, 1996.

Digital Media Monthly, Aug., 1996 (excerpt re Highwater FBI).

Digimarc Press Releases (various), 1996–1998.

Simone, "A Digita Watermark for Images," PC Magazine Dec. 18, 1996.

"Copyright Protection for Digital Images, Digital Fingerprinting from FBI," Highwater FBI brochure, 1995, 4 pages.

"Highwater FBI Limited Presentation, Image Copyright Protection Software," FBI Ltd brochure, Jul. 1995, 17 pages.

* cited by examiner

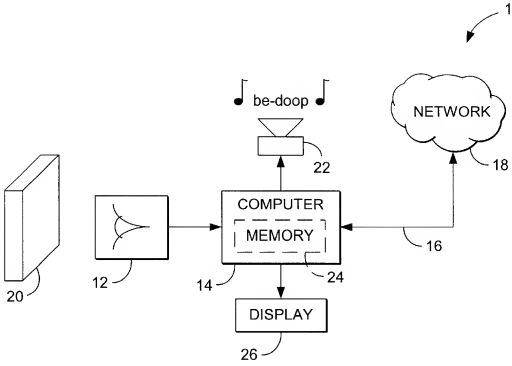

10
be-doop
NETWORK
22
18
COMPUTER
MEMORY
16
12
14
24
20
DISPLAY
26

FIG. 1

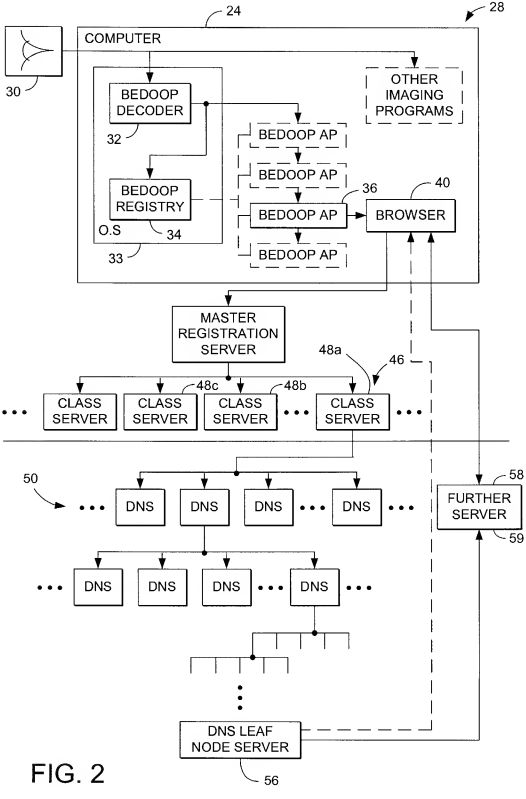

24
28
COMPUTER
30
BEDOOP DECODER
32
OTHER IMAGING PROGRAMS
BEDOOP AP
BEDOOP AP
BEDOOP REGISTRY
36
40
BEDOOP AP
BROWSER
O.S
34
33
BEDOOP AP
MASTER REGISTRATION SERVER
48a
46
48c
48b
CLASS SERVER
CLASS SERVER
CLASS SERVER
CLASS SERVER
50
DNS
DNS
DNS
DNS
58
FURTHER SERVER
59
DNS
DNS
DNS
DNS
DNS LEAF NODE SERVER
56

FIG. 2

LINKING OF COMPUTERS BASED ON OPTICAL SENSING OF DIGITAL DATA

RELATED APPLICATION DATA

This application is a continuation-in-part of copending application Ser. No. 09/130,624, filed Aug. 6, 1998, which is a continuation of application Ser. No. 08/508,083 filed on Jul. 27, 1995, (now U.S. Pat. No. 5,841,978). This application is also a continuation-in part of copending application Ser. No. 09/314,648, filed May 19, 1999 (attached as Appendix A). This application is also a continuation-in-part of copending provisional application 60/134,782, also filed May 19, 1999 (attached as Appendix B). This application is also a continuation-in-part of copending application Ser. No. 09/292,569, filed Apr. 15, 1999, which claims priority to application Ser. No. 60/082,228, filed Apr. 16, 1998.

FIELD OF THE INVENTION

The present invention relates optical user interfaces that sense digitally-encoded objects. The invention further relates to systems using such optical interfaces to control computers, and to navigate over or act as portals on networks.

BACKGROUND AND SUMMARY OF THE INVENTION

"Bedoop." That might be the sound that someone might hear as they lazily place a magazine advertisement in front of their desktop camera. Magically, the marketing and sales web site associated with the ad is displayed on their computer. More information? Want to buy now? Look at the full product line? No problem.

"Bedoop." That might be the same sound when that same someone places their credit card in front of their desktop camera. Instantly, the product displayed on the web page is purchased. Behind the scenes, a secure purchase link is initiated, transmitting all requisite information to the vendor. Twist the credit card clockwise and the purchaser chooses overnight delivery.

So goes an exemplary embodiment of the invention further described in this application. Though this example is rather specific, it nevertheless alludes to an indescribably vast array of applications possible when a digital camera or other optical sensing device is turned into a general purpose user interface device with an intuitive power that very well might rival the mouse and the keyboard.

The centerpiece of the invention is that an object or paper product so-scanned contains digital information that can be quickly read and acted upon by an appropriately configured device, computer or appliance. The preferred embodiment envisions that this digital information is aesthetically hidden on objects. These objects have been previously and proactively marked with the digital information, using any of the broad ranges of printing and processing techniques which are available on the market and which are widely described in the open literature and patent literature surrounding digital watermarking.

Be this as it may, though the invention concentrates on flat object applications wherein the digital information is often imperceptibly integrated into the object, it is certainly not meant to be so limited. Objects can be three dimensional in nature and the information more visually overt and/or preexisting (i.e., not "pro-actively" embedded, or not even be "digital," per se). Different implementation considerations attach to these variants. Likewise, though the bulk of this disclosure concentrates on objects which have some form of digital message attached thereto, some aspects of the invention may apply to objects which have no such thing, where the prior arts of pattern recognition and gestural input can be borrowed in combination with this invention to effect yet a broader array of applications.

"Bedoop." The sound that a refrigerator might make, outfitted with a simple camera/processor unit/net connection, as the ten year old holds up the empty milk carton and a ping goes out to the local grocery store, adding the item to an accumulating delivery list. The sound that might be heard echoing over and over inside Internet cafes as heretofore computerphobes take their first skeptical steps onto the world wide web. The sound heard at the fast food counter as the repeat customer holds up their sandwich card ticking off their latest meal, hoping for the sirens to go off for a $500 prize given to the lucky customer of the week. Blue sky scenarios abound.

This invention is therefore about powerful new user interfaces to computers involving optical input. These new user interfaces extend into the everyday world in ways that a mouse and keyboard never could. By enabling everyday objects to communicate their identities and functions to ever-attendant devices, not only will the world wide web be given an entirely new dimension, but basic home and office computing may be in store for some fundamental advances as well.

These and a great many other features of the present invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a block diagram showing one embodiment of the present invention.

FIG. **2** is another block diagram showing an embodiment of the present invention.

DETAILED DESCRIPTION

Basically, the technology detailed in this disclosure may be regarded as enhanced systems by which users can interact with computer-based devices. Their simple nature, and adaptability for use with everyday objects (e.g., milk cartons), makes the disclosed technology well suited for countless applications.

Due to the great range and variety of subject matter detailed in this disclosure, an orderly presentation is difficult to achieve. As will be evident, many of the topical sections presented below are both founded on, and foundational to, other sections. For want of a better rationale, the sections are presented below in a more or less random order. It should be recognized that both the general principles and the particular details from each section find application in other sections as well. To prevent the length of this disclosure from ballooning out of control, the various permutations and combinations of the features of the different sections are not exhaustively detailed. The inventors intend to explicitly teach such combinations/permutations, but practicality requires that the detailed synthesis be left to those who ultimately implement systems in accordance with such teachings.

Basic Principles—Refrigerators and Clutter

Referring to FIG. **1**, a basic embodiment 10 of the present invention includes an optical sensor **12**, a computer **14**, and a network connection **16** to the internet **18**. The illustrated optical sensor **12** is a digital camera having a resolution of

320 by 200 pixels (color or black and white) that stares out, grabbing frames of image data five times per second and storing same in one or more frame buffers. These frames of image data are analyzed by a computer **14** for the presence of Bedoop data. (Essentially, Bedoop data is any form of digital data encoding recognized by the system **10**—data which, in many embodiments, initiates some action.) Once detected, the system responds in accordance with the detected Bedoop data (e.g., by initiating some local action, or by communication with a remote computer, such as over the internet, via an online service such as AOL, or using point-to-point dial-up communications, as with a bulletin board system.

Consider the milk carton example. The artwork on a milk carton can be adapted to convey Bedoop data. In the preferred embodiment, the Bedoop data is steganographically encoded (e.g., digitally watermarked) on the carton. Numerous digital watermarking techniques are known—all of which convey data in a hidden form (i.e., on human inspection, it is not apparent that digitally encoded data is present). Exemplary techniques operate by slightly changing the luminance, or contours, of selected points on artwork or text printed on the carton, or splatter tiny droplets of ink on the carton in a seemingly random pattern. Each of these techniques has the effect of changing the local luminance at areas across the carton—luminance changes that can be detected by the computer **14** and decoded to extract the encoded digital data. In the case of a milk carton, the data may serve to identify the object as, e.g., a half gallon carton of Alpenrose brand skim milk.

The FIG. **1** apparatus can be integrated into the door of a refrigerator and used to compile a shopping list. Milk cartons, and other Bedoop-encoded packaging **20**, can be held up the optical sensor. When the computer **14** detects the presence of Bedoop data and successfully decodes same, it issues a confirmation tone ("be-doop") from a speaker or other audio transducer **22**. The computer then adds data identifying the just-detected object to a grocery list. This list can be maintained locally (in disk storage, non-volatile RAM **24**, or the like in the refrigerator, or elsewhere in the home), or remotely (e.g., at a server located at a user-selected grocery, or elsewhere). In either event, the list is desirably displayed on a display in the user's home (e.g., an LCD screen **26** built into the front of the appliance). Conventional user interface techniques can be employed permitting the user to scroll through the displayed list, delete items as desired, etc.

Periodically, the listed groceries can be purchased and the list cleared. In one embodiment, the list is printed (either at the home or at the grocery), and the user walks the grocery aisles and purchases same in the conventional manner. In another embodiment, the grocer pulls the listed items from the shelves (in response to a user request conveyed by the internet or telephone, or by a gesture as hereafter detailed). Once the list has been pulled, the grocer can alert the user that the groceries are available for pickup (again, e.g., by internet or telephone message), or the grocer can simply deliver the groceries directly to the user's home. Naturally, on-line payment mechanisms can be employed if desired.

Consider a wholly unrelated Bedoop application. An Excel spreadsheet is printed onto paper, and the paper becomes buried in a stack of clutter on an office worker's desk. Months later the spreadsheet again becomes relevant and is dug out of the stack. Changes need to be made to the data, but the file name has long-since been forgotten. The worker simply holds the dug-out page in front of a camera associated with the desktop computer. A moment later, the electronic version of the file appears on the worker's computer display.

When the page was originally printed, tiny droplets of ink or toner were distributed across the paper in a pattern so light as to be essentially un-noticeable, but which steganographically encoded the page with a plural-bit binary number (e.g., 64 bits). A database (e.g., maintained by the operating system, the Excel program, the printer driver, etc.) stored part of this number (e.g., 24 bits, termed a Univeral Identifier or UID) in association with the path and file name at which the electronic version of the file was stored, the page number within the document, and other useful information (e.g., author of the file, creation date, etc.).

The steganographic encoding of the document, and the updating of the database, can be performed by the software application (e.g., Excel). This option can be selected once by the user and applied thereafter to all printed documents (e.g., by a user selection on an "Options" drop-down menu), or can be presented to the user as part of the Print dialog window and selected (or not) for each print job.

When such a printed page is later presented to the camera, the computer automatically detects the presence of the encoded data on the page, decodes same, consults the database to identify the file name/location/page corresponding to the UID data, and opens the identified file to the correct page (e.g., after launching Excel). This application is one of many "paper as portal" applications of the Bedoop technology.

The foregoing are but two of myriad applications of the technology detailed herein. In the following discussion a great many other applications are disclosed (some groundbreaking, a few gimmicky). However, regardless of the length of the specification, it is possible only to begin to explore a few of the vast ramifications of this technology.

A few more details on the basic embodiments described above may be helpful before delving into other applications.

Optics

For any system to decode steganographically encoded data from an object, the image of the object must be adequately focused on the digital camera's CCD (or other) sensor. In a low cost embodiment, the camera has a fixed nominal focal length, e.g., in the range of 6-24 inches (greater or lesser lengths can of course be used). Since the camera is continuously grabbing and analyzing frames of data, the user can move the object towards- or away- from the sensor until the decoder succeeds in decoding the steganographically encoded data and issues a confirming "Bedoop" audio signal.

In more elaborate embodiments, known auto-focusing technology can be employed.

In still other embodiments, the camera (or other sensor) can be equipped with one or more auxiliary fixed-focus lenses that can be selectively used, depending on the particular application. Some such embodiments have a first fixed focused lens that always overlies the sensor, with which one or more auxiliary lenses can be optically cascaded (e.g., by hinge or slide arrangements). Such arrangements are desirable, e.g., when a camera is not a dedicated Bedoop sensor but also performs other imaging tasks. When the camera is to be used for Bedoop, the auxiliary lens is positioned (e.g., flipped into) place, changing the focal length of the first lens (which may by unsuitably long for Bedoop purposes, such as infinity) to an appropriate Bedoop imaging range (such as one foot).

Other lens-switching embodiments do not employ a fixed lens that always overlies the sensor, but instead employ two or more lenses that can be moved into place over the sensor. By selecting different lenses, focal lengths such as infinity, six feet, and one foot can be selected.

In all such arrangements, it is desirable (but not essential) that the steganographically-encoded portion of the object being imaged fills a substantial part of the image frame. The object can be of various sizes, e.g., an 10 by 12 inch front panel of a cereal box, or a proof of purchase certificate that is just one inch square. To meet this requirement, small objects will obviously need to be placed closer to the camera than large objects. The optics of the system can be designed, e.g., by selection of suitable aperture sizing and auxiliary lighting (if needed), to properly image objects of various sizes within a range of focal distances.

Some embodiments avoid issues of focal distances and identifying the intended object by constraining the size of the object and/or its placement. An example is a business card reader that is designed for the sole task of imaging business cards. Various such devices are known.

Decoding/Encoding

The analysis of the image data can be accomplished in various known ways. Presently, most steganographic decoding relies on general purpose microprocessors that are programmed by suitable software instructions to perform the necessary analysis. Other arrangements, such as using dedicated hardware, reprogrammable gate arrays, or other techniques, can of course be used.

The steganographic decoding process may entail three steps. In the first, the object is located. In the second, the object's orientation is discerned. In the third, the Bedoop data is extracted from the image data corresponding to the Bedoop object.

The first step, object location, can be assisted by various clues. One is the placement of the object; typically the center of the image field will be a point on the object. The surrounding data can then be analyzed to try and discern the object's boundaries.

Another location technique is slight movement. Although the user will typically try to hold the object still, there will usually be some jitter of the Bedoop object within the image frame (e.g., a few pixels back and forth). Background visual clutter, in contrast, will typically be stationary. Such movement may thus be sensed and used to identify the Bedoop object from within the image data.

Still another object-location clue is object shape. Many Bedoop objects are rectangular in shape (or trapezoidal as viewed by the camera). Straight edge boundaries can thus be used to define an area of likely Bedoop data.

Color is a further object identification clue that may be useful in some contexts.

Yet another object location clue is spatial frequency. In imaging systems with well defined focal zones, undesired visual clutter may be at focal distances that results in blurring. The Bedoop object, in contrast, will be in focus and may be characterized by fine detail. Analyzing the image data for the high frequencies associated with fine detail can be used to distinguish the intended object from others.

Characteristic markings on the object (as discussed below in connection with determining object orientation), can also be sensed and used in locating the object.

Once the Bedoop object has been located within the image data, masking can be applied (if desired) to eliminate image data not corresponding to the intended object.

The second step in the decoding process—determining orientation of the Bedoop data—can likewise be discerned by reference to visual clues. For example, some objects include subliminal graticule data, or other calibration data, steganographically encoded with the Bedoop data to aid in determining orientation. Others can employ overt markings, either placed for that sole purpose (e.g. reference lines or fiducials), or serving another purpose as well (e.g. lines of text), to discern orientation. Edge-detection algorithms can also be employed to deduce the orientation of the object by reference to its edges.

Some embodiments filter the image data at some point in the process to aid in ultimate Bedoop data extraction. One use of such filtering is to mitigate image data artifacts due to the particular optical sensor. For example, CCD arrays have regularly-spaced sensors that sample the optical image at uniformly spaced discrete points. This discrete sampling effects a transformation of the image data, leading to certain image artifacts. An appropriately configured filter can mitigate the effect of these artifacts.

(In some arrangements, the step of determining the orientation can be omitted. Business card readers, for example, produce data that is reliably free of artifacts and is of known scale. Or the encoding of the Bedoop data can be effected in such a way that renders it relatively immune to certain distortion mechanisms. For example, while the presently-preferred encoding arrangement operates on a 2D grid basis, with rows and columns of data points, the encoding can alternatively be done on another basis (e.g., a rotationally-symmetric form of encoding, such as a 2D bar-code, so that rotational state of the image data can be ignored). In still other embodiments, the orientation-determining step can be omitted because the decoding can readily proceed without this information. For example decoding which relies on the Fourier-Mellin transform produces data in which scale and rotation can be ignored.)

Once the orientation of the object is discerned, the image data may be virtually re-registered, effectively mapping it to another perspective (e.g., onto a rectilinear image plane). This mapping can employ known image processing techniques to compensate, e.g., for rotation state, scale state, differential scale state, and X-Y offset, of the original Bedoop image data. The resulting frame of data may then be more readily processed to extract the steganographically-encoded Bedoop data.

In the preferred embodiment, after the image data is remapped into rectilinear planar form, subliminal graticule data is sensed that identifies the locations within the image where the binary data is encoded. Desirably, the binary data is redundantly encoded, e.g., in 8×8 patch blocks. Each patch comprises one or more pixels. (The patches are typically square, and thus contain 1, 4, 9, or 16, etc. pixels.) The nominal luminance of each patch before encoding (e.g., artwork pre-existing on the object) is slightly increased or decreased to encode a binary "1" or "0." The change is slight enough to be generally imperceptible to human observers, yet statistically detectable from the image data—especially if several such blocks are available for analysis. Preferably, the degree of change is adapted to the character of the underlying image, with relatively greater changes being made in regions where the human eye is less likely to notice them. Each block thus encoded can convey 64 bits of data. The encoding of such blocks in tiled fashion across the object permits the data to be conveyed in robust fashion.

Much of the time, of course, the Bedoop sensor is staring out and grabbing image frames that have no Bedoop data. Desirably, the detection process includes one or more checks to assure that Bedoop data is not wrongly discerned from non-Bedoop image data. Various techniques can be employed to validate the decoded data, e.g., error detecting codes can be included in the Bedoop payload and checked to confirm correspondence with the other Bedoop payload. Likewise, the system can confirm that the same Bedoop data is present in different tiled excerpts within the image data, etc.

(Details of the preferred encoding techniques are further detailed in co-pending applications Ser. No. 09/293,601, filed Apr. 15, 1999, entitled METHODS AND DEVICES FOR RECOGNIZING BANKNOTES AND RESPONDING ACCORDINGLY, Ser. No. 09/127,502, filed Jul. 31, 1998, and U.S. Pat. No. 5,862,260.)

Data Structures, Formats, Protocols, and Infrastructures

In an exemplary system, the Bedoop data payload is 64 bits. This payload is divided into three fields CLASS (12 bits), DNS (24 bits) and UID (24 bits). (Other payload lengths, fields, and divisions, are of course possible, as is the provision of error-checking or error-correcting bits.)

Within the above-described eight patch-by-eight patch data block, the bits are ordered row by row, starting with the upper left patch. The first 12 bits are the CLASS ID, followed by 24 bits of DNS data followed by 24 bits of UID data. (In other embodiments, the placement of bits comprising these three fields can be scrambled throughout the block.)

Briefly, the CLASS ID is the most rudimentary division of Bedoop data, and may be analogized, in the familiar internet taxonomy, to the limited number of top level domains (e.g., .com, .net, .org, .mil, .edu, .jp, .de, .uk, etc.). It is basically an indicator of object type. The DNS ID is an intermediate level of data, and may be analogized to internet server addresses (e.g., biz.yahoo, interactive.wsj, etc.). The UID is the finest level of granularity, and, can roughly be analogized to internet pages on a particular server (e.g., edition/current/summaries/front.htm, daily/home/default.hts, etc.).

Generally speaking, the CLASS ID and DNS ID, collectively, indicate to the system what sort of Bedoop data is on the object. In the case of Bedoop systems that rely on remote servers, the CLASS and DNS IDs are used in identifying the server computer that will respond to the Bedoop data The UID determines precisely what response should be provided.

In the case of a refrigerator Bedoop system, what happens if an object with an unfamiliar CLASS/DNS ID data is encountered? The system can be programmed not to respond at all, or to respond with a raspberry-like sound (or other feedback) indicating "I see a Bedoop object but don't know what to do with it."

Most systems will be able to respond to several classes of Bedoop objects. Simple software-based systems can compare the CLASS/DNS ID (and optionally the UID) to fixed values, and can branch program execution to corresponding subroutines. Likewise, hardware-based systems can activate different circuitry depending on the detected CLASS/DNS ID.

In the case of a computer equipped with a Bedoop input device (e.g., a Sony VAIO PictureBook laptop with built-in camera), the operating system's registry database can be employed to associate different application programs with different CLASS/DNS IDs (just as the .XLS and .DOC file extensions are commonly associated by existing operating system registries to invoke Microsoft Excel and Word software applications, respectively). When a new Bedoop application is installed, it logs an entry in the registry database indicating the CLASS/DNS ID(s) that it will handle. Thereafter, when an object with such a CLASS/DNS ID is encountered, the operating system automatically launches the corresponding application to service the Bedoop data in an appropriate manner.

Sometimes the computer system may encounter a Bedoop object for which it does not have a registered application program. In such case, a default Bedoop application can be invoked. This default application can, e.g., establish an internet link to a remote server computer (or a network of such computers), and can transmit the Bedoop data (or a part of the Bedoop data) to that remote computer. The remote server can undertake the response itself, it can instruct the originating computer how to respond appropriately, or it can undertake some combination of these two responses. (Such arrangements are further considered below.)

FIG. **2** shows an illustrative architecture employing the foregoing arrangement.

At a local Bedoop system **28** (which may be implemented, for example, using a conventional personal computer **29**), a camera, scanner, or other optical sensor **30** provides image data to a decoder **32** (which may be implemented as a software component of the operating system **33**). The decoder **32** analyzes the image data to discern the plural-bit Bedoop data. The CLASS ID of this Bedoop data is applied to a Bedoop registry **34**. The registry responds by identifying and launching a local Bedoop application **36** designed to service the discerned Bedoop data.

Sometimes the system **28** may encounter a Bedoop object for which several different responses may be appropriate. In the case of a printed office document, for example, one response may be as described above—to present the electronic version of the file on a computer, ready for editing. But other responses may also be desired, such as writing an email message to the author of the printed document, with the author's email address already specified in the message address field, etc.

Such different responses may be handled by different Bedoop applications, or may be options that are both provided by a single Bedoop application. In the former case, when the CLASS/DNS IDs are decoded and provided to the operating system, the registry indicates that there are two (or more) programs that might be invoked. The operating system can then present a dialog box to the user inviting the user to specify which form of response is desired. Optionally, a default choice can be made if the user doesn't specify within a brief period (e.g., three seconds). The operating system can then launch the Bedoop application corresponding to the chosen response.

A similar arrangement can be employed if a single Bedoop application can provide both responses. In such case the operating system launches the single Bedoop application (since there is no ambiguity to be resolved), and the application presents the choice to the user. Again, the user can select, or a default choice can be automatically made.

In the just-described situations, the user can effect the choice by using the keyboard or mouse—as with traditional dialog boxes. But Bedoop provides another, usually easier, form of interaction. The user can make the selection through the optical sensor input. For example, moving the object to the right can cause a UI button on the right side of the dialog box to be selected; moving the object to the left can cause a UI button on the left side of the dialog box to be selected; moving the object towards the camera can cause the selected button to be activated. Many other such techniques are possible, as discussed below.

If the registry **34** does not recognize, or otherwise does not know how to respond to Bedoop data of that particular CLASS/DNS, the registry launches a default Bedoop client application. This client application, in turn, directs a web browser **40** on the local Bedoop system **28** to communicate with a remote master registration server computer **42**. The local computer forwards the Bedoop data to this master server. The master server **42** examines the CLASS ID, and forwards the Bedoop data (directly, or through intervening servers) to a corresponding CLASS server **44**. (A single

server may handle Bedoop data of several classes, but more typically there is a dedicated server for each CLASS.)

Each CLASS server **44** serves as the root of a tree **46** of distributed DNS servers. A DNS server **48***a*, for example, in a first tier **50** of the DNS server tree, may handle Bedoop data having DNS IDs beginning with "000." Likewise, DNS server **48***b* may handle Bedoop data having DNS IDs beginning with "001," etc., etc.

Each DNS server in the first tier **50** may, in turn, route Bedoop data to one of 8 servers in a second tier of the tree, in accordance with the fourth-through sixth bits of the DNS data. The tree continues in this fashion until a terminal level of DNS leaf node servers **56**.

Ultimately, Bedoop data routed into this network reaches a DNS leaf node server **56**. That leaf node server may handle the Bedoop data, or may redirect the local Bedoop system to a further server **58** that does so. That ultimate server—whether a DNS leaf node server or a further server—can query the local Bedoop system for further information, if necessary, and can either instruct the local Bedoop system how to respond, or can undertake some or all of the response itself and simply relay appropriate data back to the local Bedoop system.

In arrangements in which the local Bedoop system is redirected, by the DNS leaf node server, to a further server that actually handles the response, access to the further server may be through a port **59** (e.g., a special URL) tailored to receipt of Bedoop data.

In a typical implementation, most or all of the servers are mirrored, or otherwise replicated/redundant, so that failure of individual computers does not impair operation of the system.

Caching can be provided throughout the trees of servers to speed responses. That is, responses by leaf nodes for certainly commonly-encountered CLASS/DNS IDs can be temporarily stored earlier in the tree(s). Bedoop data, propagating through the server network, can prompt a response from an intermediate server if there is a cache hit.

If desired, Bedoop traffic through the above-detailed server trees can be monitored to collect demographic and statistical information as to what systems are sending what Bedoop data, etc. One use of such information is to dynamically reconfigure the DNS network to better balance server loads, to virtually relocate DNS resources nearer regions of heavy usage, etc. Another use of such information is for marketing purposes, e.g., to promote certain Bedoop features and applications within user groups (e.g., internet domains) that seem to under-utilize those features.

Within certain user networks that are linked to the internet, e.g., corporate networks, Bedoop data that isn't handled within the originating Bedoop system may first be routed to a Bedoop name server within the corporate network. That server will recognize certain types of Bedoop data, and know of resources within the corporate network suitable for handling same. Referral to such resources within the corporate network will be made, where possible. These resources (e.g., corporate servers) may respond to Bedoop data in a way customized to the corporate preferences. If the corporate Bedoop name server does not know of a resource within the corporate network that can respond to the Bedoop data, the corporate name server then routes the data to the public Bedoop network described above. (Such referral can be to the master registration server or, to the extent the corporate name server knows the addresses of appropriate servers within the DNS server tree, or of the further servers to which DNS servers may point for certain Bedoop data, it can redirect the local Bedoop system accordingly.)

In typical rich Bedoop implementations, local systems may have libraries of Bedoop services, applications, or protocols. Some may be unique to that computer. Others may be commonly available on all computers. Some may be highly secure, employing encryption and/or anti-hacking measures, or data protocols that are not generally recognized. Others may be shareware, or the result of open-source programming efforts.

Greeting Cards, Birthday Cards, Etc.

In accordance with a further embodiment of the invention, greeting cards and the like are encoded (e.g., by texturing, printing, etc.) with Bedoop data. On receiving such a card, a recipient holds it in front of the image capture device on a laptop or other computer. The computer responds by displaying an internet web page that has a stock- or customized-presentation (image, video, audio-video, etc.) to complement that presented on the greeting card.

The web site presentation can be personalized by the sender (e.g., with a text message, recent family photographs, etc.), either at the point of card sale, or sometime after the card is purchased. In the latter case, for example, the card can be serialized. After taking the card home, the purchaser can visit the card vendor's web site and enter the card serial number in an appropriate user interface. The purchaser is then presented with a variety of simple editing tools to facilitate customization of the web greeting. When the sender is finished designing the web greeting, the finished web page data is stored (by software at the vendor's web site) at a site corresponding to the serial number.

When the card is received by a recipient and held in front of a Bedoop sensor, CLASS, DNS, and UID data is decoded from the card. The CLASS and DNS data are used to navigate the earlier-described server network to reach a corresponding DNS leaf node server (perhaps maintained by the Hallmark greeting card company). That leaf node server indexes a table, database, or other data structure with the UID from the Bedoop data, and obtains from that data structure the address of an ultimate web site—the same address at which the web greeting customized by the sender was stored. That address is provided by the DNS leaf node server back to the local computer, with instructions that the web page at that address be loaded and displayed (e.g., by HTML redirection). The local computer complies, presenting the customized web greeting to the card recipient.

In the just-described embodiment, in which a pre-encoded card is purchased by a sender and the web-display is then customized, the address of the web site is typically determined by the card vendor. But this need not be the case. Likewise, the card need not be "purchased" in the typical, card-shop fashion.

To illustrate the foregoing alternatives, consider the on-line acquisition of a greeting card, e.g., by visiting a web site specializing in greeting cards. With suitable user-selection (and, optionally, customization), the desired card can be printed using an inkjet or other printer at the sender's home. In such case, the Bedoop data on the card can be similarly customized. Instead of leading to a site determined by the card vendor, the data can lead to the sender's personal web page, or to another arbitrary web address.

To effect such an arrangement, the sender must arrange for a DNS leaf node server to respond to a particular set of Bedoop data by pointing to the desired web page. While individuals typically will not own DNS servers, internet service providers commonly will. Just as AOL provides simple tools permitting its subscribers to manage their own modest web pages, internet service providers can likewise provide simple tools permitting subscribers to make use of

DNS leaf node servers. Each subscriber may be assigned up to 20 UIDs (under a particular CLASS and DNS). The tools would permit the users to define a corresponding web address for each UID. Whenever a Bedoop application led to that DNS leaf node server, and presented one of those UIDs, the server would instruct the originating computer to load and present the web page at the corresponding web address **58**.

Prior to customizing the greeting card, the sender uses the tool provided by the internet service provider to store the address of a desired destination web address in correspondence with one of the sender's available UIDs. When customizing the greeting card, the sender specifies the Bedoop data that is to be encoded, including the just-referenced UID. The greeting card application encodes this data into the artwork and prints the resulting card. When this card is later presented to a Bedoop system by the recipient, the recipient's system loads and displays the web page specified by the sender.

Commerce in Bedoop Resources

In the just-described arrangement, internet service providers make available to each subscriber a limited number of UIDs on a DNS server maintained by the service. Business enterprises typically need greater Bedoop resources, such as their own DNS IDs (or even their own CLASS ID(s).

While variants of the Bedoop system are extensible to provide an essentially unlimited number of CLASS IDs and DNS IDs, in the illustrated system these resources are limited. Public service, non-profit, and academic applications should have relatively generous access to Bedoop resources, either without charge or for only a modest charge. Business enterprises, in contrast, would be expected to pay fees to moderate their potentially insatiable demand for the resources. Small businesses could lease blocks of UIDs under a given CLASS/DNS ID. Larger businesses could acquire rights to entire DNS IDs, or to entire CLASS IDs (at commensurately greater fees).

Web-based systems for assigning DNS IDs (and CLASS IDs) can be modeled after those successfully used by Internic.com, and now Networksolutions.com, for registration of internet domains. The user fills out a web-based form with names, addresses, and billing information; the system makes the necessary changes to all of the hidden system infrastructure—updating databases, routing tables, etc., in servers around the world.

Controlled-Access ID

Just as the above-described embodiment employed an ink-jet printer to produce a customized-Bedoop greeting card, the same principles can likewise be applied to access-control objects, such as photo-IDs.

Consider an employment candidate who will be interviewing at a new employer. The candidate's visit is expected, but she is not recognized by the building's security personnel. In this, and many other applications, arrangements like the following can be used:

The employer e-mails or otherwise sends the candidate an access code. (The code can be encrypted for transmission.) The code is valid only for a certain time period on a given date (e.g., 9:00 a.m. –11:00 a.m. on Jun. 29, 1999).

Upon receipt of the access code, the candidate downloads from the web site of the state Department of Motor Vehicles the latest copy of her driver's license photo. The DMV has already encoded this photo with Bedoop data. This data leads to a state-run DNS leaf node server **56**. When that server is presented with a UID decoded from a photograph, the server accesses a database and returns to the inquiring computer a text string indicating the name of the person depicted by the photograph.

The candidate incorporates this photo into an access badge. Using a software application (which may be provided especially for such purposes, e.g., as part of an office productivity suite), the photo is dragged into an access badge template. The access code emailed from the employer is also provided to this application. On selecting "Print," an ink-jet printer associated with the candidate's computer prints out an access badge that includes her DMV photo and her name, and is also steganographically encoded in accordance with the employer-provided access code.

The name printed on the badge is obtained (by the candidate's computer) from the DMV's DNS server, in response to Bedoop data extracted from the photograph. (In this application, unlike most, the photograph is not scanned as part of a Bedoop process. Instead, the photograph is already available in digital form, so the Bedoop decoding proceeds directly from the digital representation.)

For security purposes, the access code is not embedded using standard Bedoop techniques. Instead, a non-standard format (typically steganographic) is employed. The embedding of this access code can span the entire face of the card, or can be limited to certain regions (e.g., excluding the region occupied by the photograph).

On the appointed day the candidate presents herself at the employer's building. At the exterior door lock, the candidate presents the badge to an optical sensor device, which reads the embedded building access code, checks it for authenticity and, if the candidate arrived within the permitted hours, unlocks the door.

Inside the building the candidate may encounter a security guard. Seeing an unfamiliar person, the guard may visually compare the photo on the badge with the candidate's face. Additionally, the guard can present the badge to a portable Bedoop device, or to one of many Bedoop systems scattered through the building (e.g., at every telephone). The Bedoop system extracts the Bedoop data from the card (i.e., from the DMV photograph), interrogates the DMV's DNS server with this Bedoop data, and receives in reply the name of the person depicted in the photograph. (If the Bedoop system is a telephone, the name may be displayed on a small LCD display commonly provided on telephones.)

The guard checks the name returned by the Bedoop system with the name printed on the badge. On seeing that the printed and Bedoop-decoded names match (and optionally checking the door log to see that a person of that name was authorized to enter and did so), the security guard can let the candidate pass.

It will be recognized that the just-described arrangement offers very high security, yet this security is achieved without the candidate ever previously visiting the employer, without the employer knowing what the candidate looks like, and by use of an access badge produced by the candidate herself.

Variants of such home-printed badge embodiments find numerous applications. Consider purchasing movie- or event-tickets over the web. The user can print an access ticket that has an entry code embedded therein. On arriving at the theater or event, the user presents the ticket to an optical scanning device, which decodes the entry code, checks the validity of same, authorizes the entry, and marks that entry code as having been used (preventing multiple uses of tickets printed with the same code).

Ink-Jet Printing

In the foregoing discussions, reference has been made to use of ink-jet printing as a means for providing steganographically encoded indicia on substrates. The following discussion expands on some of the operative principles.

The basic physics and very low level analog electronic operation of ink-jet printers (sometimes termed bubble-jet printers) are ideally suited to support very-light-tint background digital watermarking on any form of substrate. (Watermarking through apparent "tinting" of substrates is discussed in copending application Ser. No. 09/127,502.) In general, the statement, "if you can print it with an ink jet printer, you can watermark it" is largely accurate, even for (perhaps especially for) simple text documents. Indeed, there is a degree of flexibility and control in the ink-jet printing realm that is not as generally available in more traditional printing technologies, such as commercial offset printing and other plate-based technologies. (This is not to say that ink-jet has better quality than plate-based technologies; it has more to do with the statistics of ink droplets than anything else.) Heavier tint backgrounds are possible as well, where the continuum ranges from very light background tinting, where the casual observer will see "white paper," all the way through heavily inked patterned backgrounds, and photographs themselves, and everything in between.

In some embodiments, the ink-jet driver software is modified to provide lower-level control of individual droplet emission than is provided in existing printer drivers, which are naturally optimized for text and graphics. In some such embodiments, the "watermarking" print mode is another option from which the user can select (e.g., in addition to High Quality, Econo-Fast, etc.), or the selection can be made automatically by application software that is printing watermarked data.

In more sophisticated embodiments, the watermark data is applied to the printer driver software independently of the other image/text data. The printer driver is arranged to eject droplets in the usual print density for the image/text data, and at a more accurately-controlled, finer density for the separately-applied watermark data. (The latter may be effected as a slight modulation signal on the former.) This arrangement provides for essentially transparent integration into existing printer environments—no one need worry about the watermarking capability except the software applications that specifically make use of same.

Consumer Marking of Web-Based Materials

Various items of printed media can originate off the web, yet be printed at home. Examples include movie tickets, coupons, car brochures, etc. Bedoop data can be added, or modified, by the software application or by the printer driver at the time of printing. (Alternatively, the Bedoop data can be customized to correspond to the user before being downloaded to the user's system for printing.)

One advantage to Bedoop-encoding printed images locally, as opposed to Bedoop-encoding the image files prior to downloading for local printing, is that the encoding can be tailored in accordance with the particular properties of the local printer (e.g., to increase robustness or decrease visibility)—properties not generally known to a remote server.

In one particular example, the UID field in the Bedoop data can be written with a value that serves as an index to a database of user profiles, permitting later systems to which the printed item is presented to personalize their response in accordance with the profile data.

In another example, the UID field serves an authentication purpose, e.g., to verify that the printed medium actually was printed at a particular place, or by a particular user or at a particular time.

Coffee Mug

At retail coffee outlets, customers commonly order the same drink day after day ("half-decaf, short, skinny latte"). Some customers present personal coffee mugs to the cashier, preferring the sensation of ceramic or metal to paper, and avoiding the trash/recycle dilemma.

The drinker's "regular" order can be Bedoop-encoded either on the mug itself or, more commonly, on an adhesive label applied to the mug. The encoding can be in addition to other aesthetic imagery (e.g., artwork or a photo), or the marking can be purely data. Labels the size of postage stamps may be used.

On handing the mug to the cashier, the customer can simply say "the regular." The cashier passes the mug in front of the optical scanning device of a Bedoop system associated with the cash register. The system steganographically decodes the data and provides the corresponding order ("half-decaf, short, skinny latte"), either textually or audibly (e.g., by a voice synthesizer) to the cashier or the barrista. The cash register system also knows the current price of the requested drink, and rings up the charge accordingly.

Labels of the type described can be available to the cashier on pre-printed rolls, just as with other adhesive stickers, or can be printed on-demand. (Small label printers may be best suited in the latter case, given space constraints in retail outlets.) Customers ordering drinks for personal mugs may be invited to take a label corresponding to their just-ordered drink and apply it to their mug for future use.

In variants on this basic theme, the mug label can be further encoded (or a supplemental label can be provided and encoded) with electronic payment information, such as the customer's credit card number, or the number of a debit account maintained by the coffee merchant for that customer. When the mug is scanned for the drink order, the system likewise detects the payment information and charges the corresponding fee to the appropriate account. (For security reasons, the system may be arranged so that the mug cannot be used to authorize more than, say $5 of coffee drink purchases per day.)

In another variant on this theme, the system maintains an electronic log of coffee purchases made by the customer and, in accordance with then-prevailing marketing considerations, rewards the customer with a free drink after 8 or 12, etc., drinks have been purchased.

In still another variant on this theme, regular customers who use Bedoop-labeled mugs can participate in periodic promotions in which, for example, every N^{th} such customer is rewarded with a cash or merchandise prize. Bells go off when the N^{th} mug is scanned. (N can be a fixed number, such as 500, or can be a random number—typically within a known range or with a known mean.)

Smart Elevators

In accordance with another embodiment of the invention, a building elevator is provided with one or more optical capture devices. Each device examines monitors the contents of the elevator chamber looking for Bedoop encoded objects, such as ID badges.

On sensing a Bedoop-encoded object, the elevator can determine—among other data—the floor on which the wearer's office is located. The system can then automatically direct the elevator to that floor, without the need for the person to operate any buttons. (The elevator's button panel can be provided with a new, override button that can be operated to un-select the most recently selected floor(s), e.g., in case a user wants to travel to a different floor.) To aid in identification, the Bedoop objects (e.g., badges) can be colored a distinctive color, permitting the system to more easily identify candidate objects from other items within the optical capture devices' field of view. Or the object can be provided with a retro-reflective coating, and the elevator can

be equipped with one or more illumination sources of known spectral or temporal quality (e.g., constant infra red, or constant illumination with a single- or multi-line spectrum, or a pulsed light source of known periodicity, LEDs or semiconductor lasers, each with an associated diffuser, can be used for each the foregoing and can be paired with the image capture devices). Other such tell-tale clues can likewise be used to aid in object location. In all such cases, the optical capture device can sense the tell-tale clue(s) using a wide field of view sensor. The device can then be physically or electronically steered, and/or zoomed, to acquire a higher resolution image of the digitally-encoded object suitable for decoding.

Magazines

Magazine (and newspaper) pages can be steganographically encoded with Bedoop data to provide another "paper as portal" experience. As with the earlier described office document case, the encoded data yields an address to a computer location (e.g., a web page) having the same, or related, content.

In one exemplary embodiment, the blank magazine page stock is Bedoop-encoded prior to printing. The watermarking can be performed by high speed ink-jet devices, which splatter a fine pattern of essentially imperceptible ink droplets across each page. Each page can be differently watermarked so that, on decoding, page 21 of a magazine can be distinguished from page 22 of the same magazine (and page 106 of the Jun. 21, 1999, issue can be distinguished from page 106 of the Jun. 28, 1999, issue). If desired, each page can be further segregated into regions—either in accordance with the actual boundaries of articles that will later be printed on the pages, or in a grid pattern, e.g., of 3 columns across by 5 rows high. Each region conveys a distinct Bedoop code, permitting different portions of the page to lead to different web data.)

After watermarking and printing, the pages thus produced are bound in the usual fashion with others to form the finished magazine. (Not all pages in the magazine need to be watermarked.)

Of course, the watermarking can be effected by processes other than ink-jet printing. For example, texturing by pressure rollers is another option well suited for the large volumes of paper to be processed.

On presenting a magazine to the optical scanner device of a Bedoop-compliant computer, the computer senses the Bedoop data, decodes same, and launches a web browser to an internet address corresponding to the Bedoop data. If the magazine page is an advertisement, the internet address can provide information complementary to the advertisement. For example, if the magazine page is an advertisement for a grocery item, the Bedoop data can identify a web page on which recipes using the advertised item are presented. If the magazine page includes a photo of a tropical beach, the Bedoop data can lead to a travel web page (e.g., hosted by Expedia or other travel service) that presents fare and lodging information useful to a reader who wants to vacation at the illustrated beach. (The fare information can be customized to the reader's home airport by reference to user profile data stored on the user's computer and relayed to the web site to permit customization of the displayed page.)

The data to which the Bedoop data leads needn't be static; it can be updated on a weekly, daily, or other basis. Thus, if a months-old magazine page is presented to a Bedoop device, the resultant data can be up-to-the-minute.

In the case of advertising, the inclusion of Bedoop data increases the value of the ad to the advertiser, and so merits a higher charge to the advertiser from the magazine publisher. This higher charge may be shared with the enterprise (s) that provides the Bedoop technology and infrastructure through which the higher value is achieved.

Business Card Applications

Conventional business cards can be steganographically encoded with Bedoop data, e.g., by texturing, watermark tinting, ink-jet splattering, text steganography, etc. As with many of the earlier-described embodiments, the steganographic encoding is tailored to facilitate decoding in the presence of arbitrary rotation or scale distortion of the card introduced during scanning. (Some such techniques are shown, e.g., in applicant's related patents identified above. Various other techniques are known to artisans.)

When a recipient of a business card holds it in front of a Bedoop sensor, the operating system on the local system launches a local Bedoop application. That local Bedoop application, in turn, establishes an external internet connection to a remote business card server. The address of that server may already be known to the local Bedoop application (e.g., having been stored from previous use), or the local Bedoop system can traverse the above-described public network of DNS servers to reach the business card server.

A database on the business card name server maintains a large collection of business card data, one database record per UID. When that server receives Bedoop data from a local Bedoop system, it parses out the UID and accesses the corresponding database record. This record typically includes more information than is commonly printed on conventional business cards. Sample fields from the record may include, for example, name, title, office phone, office fax, home phone, home fax, cellular phone, email address, company name, corporate web page address, personal web page address, secretary's name, spouse's name, and birthday. This record is transmitted back to the originating Bedoop system.

The local Bedoop system now has the data, but needs further instruction from the user as to how it should be processed. Should a telephone number be dialed? Should the information be entered into a personal contact manager database (e.g., Outlook) on the local system? Etc.

In an exemplary embodiment, the local system presents the available choices to the user, e.g., by textual prompts, synthesized voice, etc. The user responds by manipulating the business card in a manner prompted by the system (e.g., move down to telephone at office; move up to telephone at home; move right to access corporate web page; move left to access personal web page; rotate left to enter certain elements from the database record (filtered in accordance with a template) into personal contact manager database, etc. The local Bedoop system responds accordingly.

Some card givers may choose to make additional information available to card recipients—information beyond that known in prior art contact-management software applications. For example, one of the choices presented by a local Bedoop system in response to presentation of a business card may be to review the card-giver's personal calendar. (The card-giver can maintain his or her personal calendar on a web-accessible computer.) By such arrangement, the card-recipient can learn when the card-giver may be found in the office, when appointments might be scheduled, etc., etc.

Typically, access to this web-calendar is not available to casual web browsers, but is accessible only in response to Bedoop data (which may thus be regarded as a form of authentication or password data).

Some users may carry several differently-encoded cards, each with a different level of access authorization (e.g., with different UIDs). Thus, some cards may access a biographical

page without any calendar information, other cards may access the same or different page with access enabled to today's calendar, or this week's calendar, only, and still other cards (e.g., the "spouse" card) may access the same or different page with access enabled for the card-giver's complete calendar. The user can distribute these different cards to different persons in accordance with the amount of personal information desired to be shared with each.

In accordance with a related embodiment, the database record corresponding to Bedoop business card data can include a "now" telephone number field. This field can be continually-updated throughout the day with the then-most-suitable communications channel to the card-giver. When the card-giver leaves home to go to the office, or leaves the office for a trip in the car, or works a week at a corporate office in another town, etc., this data field can be updated accordingly. (A pocket GPS receiver, with a wireless uplink, can be carried by the person to aid in switching the "now" number among various known possibilities depending on the person's instantaneous position.) When this database record is polled for the "now" number, it provides the then-current information.

Consider a Bedoop-enabled public telephone. To dial the phone, a business card is held in front of the Bedoop sensor (or slid through an optical scanner track). The phone interrogates the database at the business card server for the "now" number and dials that number.

To update the any of the fields stored in the database record, the card giver can use a special card that provides write-authorization privileges. This special card can be a specially encoded version of the business card, or can be another object unique to the card-giver (e.g., the card-giver's driver's license).

The reference to business cards and personal calendars is illustrative only. Going back a century, "calling cards" were used by persons whose interests were strictly social, rather than business. The just-discussed principles can be similarly applied. Teenagers can carry small cards to exchange with new acquaintances to grant access to private dossiers of personal information, favorite music, artwork, video clips, etc. The cards can be decorated with art or other indicia that can serve purposes wholly unrelated to the Bedoop data steganographically encoded therein.

Gestural Input

A Bedoop system can determine the scale state, rotation state, X-Y offset, and differential scale state, of an object by reference to embedded calibration data, or other techniques. If the scan device operates at a suitably high frame rate (e.g., five or ten frames per second), change(s) in any or all of these four variables can be tracked over time, and can serve as additional input.

In an earlier-discussed example, moving an object to the left or right in front of the Bedoop scanner caused a left- or right-positioned button in a dialog box to be selected. This is a change in the X-Y offset of the scanned object. In that earlier example, moving the object inwardly towards the camera caused the selected button to be activated. This is a change in the scale state of the scanned object.

In similar fashion, twisting the object to the left or right can prompt one of two further responses in a suitably programmed Bedoop application. (This is a change in the rotation state.) Likewise, tilting the object so that one part is moved towards or away from the camera can prompt one of two further responses in the application. (This is a change in the differential scale state.)

In the business card case just-discussed, for example, the card can be held in front of the Bedoop scanner of a computer. If the card is twisted to the left, the computer opens a web browser to a web page address corresponding to Bedoop data on the card. If the card is twisted to the right, the computer opens an e-mail template, pre-addressed to an e-mail address indicated by the card.

In other examples, twisting an object to move the right edge towards the scanner can be used to effect a right mouse click input, and twisting the object to move the right edge away from the scanner can be used to effect a left mouse click input.

Simultaneous changes in two of these four positioning variables can be used to provide one of four different inputs to the computer (e.g., (a) twisting left while moving in; (b) twisting left while moving out; (c) twisting right while moving in; and (d) twisting right while moving out). Simultaneous changes to three or all four of these variables can similarly be used to provide one of eight or sixteen different inputs to the computer.

Simultaneous manipulations of the object in two or more of these modes is generally unwieldy, and loses the simple, intuitive, feel that characterizes manipulation of the object in one mode. However, a similar effect can be achieved by sequential, rather than simultaneous, manipulation of the card in different modes (e.g., twist left, then move in). Moreover, sequential manipulations permit the same mode to be used twice in succession (e.g., move in, then move out). By such sequential manipulations of the object, arbitrarily complex input can be conveyed to the Bedoop system.

(It will be recognized that a digitally-encoded object is not necessary to the gestural-input applications described above. Any object (talisman) that can be distinguished in the image data can be manipulated by a user in the manners described above, and an appropriate system can recognize the movement of the object and respond accordingly. The provision of digital data on the object provides a further dimension of functionality (e.g., permitting the same gesture to mean different things, depending on the digital encoding of the object being manipulated), but this is not essential.

Moreover, even within the realm of digitally-encoded gestural talismans, steganographic encoding is not essential. Any other known form of optically-recognizable digital encoding (e.g., 1D and 2D bar codes, etc.) can readily be employed.

In an illustrative embodiment, a business card or photograph is used as the talisman, but the range of possible talismans is essentially unlimited.

Gestural Decoding Module

There are various ways in which the Bedoop system's decoding of gestural input can be effected. In some Bedoop systems, this functionality is provided as part of the Bedoop applications. Generally, however, the applications must be provided with the raw frame data in order to discern the gestural movements. Since this functionality is typically utilized by many Bedoop applications, it is generally preferable to provide a single set of gestural interpretation software functions (commonly at the operating system level) to analyze the frame data, and make available gestural output data in standardized form to all Bedoop applications.

In one such system, a gestural decoding module tracks the encoded object within the series of image data frames, and outputs various parameters characterizing the object's position and manipulation over time. Two of these parameters indicate the X-Y position of the object within current frame of image data. The module can identify a reference point (or several) on the object, and output two corresponding position data (X and Y). The first represents the horizontal offset

of the reference point from the center of the image frame, represented as a percentage of frame width. A two's complement representation, or other representation capable of expressing both positive and negative values, can be used so that this parameter has a positive value if the reference point is right of center-frame, and has a negative value if the reference point is left of center frame. The second parameter, Y, similarly characterizes the position of the reference point above or below center-frame (with above-being represented by a positive value). Each of these two parameters can be expressed as a seven-bit byte. A new pair of X, Y parameters is output from the gestural decoding module each time a new frame of image data is processed.

In many applications, the absolute X-Y position of the object is not important. Rather, it is the movement of the object in X and Y from frame-to-frame that controls some aspect of the system's response. The Bedoop application can monitor the change in the two above-described parameters, frame to frame, to discern such movement. More commonly, however, the gestural decoding module performs this function and outputs two further parameters, X' and Y'. The former indicates the movement of the reference point in right/left directions since the last image frame, as a percentage of the full-frame width. Again, this parameter is represented in two's complement form, with positive values representing movement in the rightward direction, and negative values representing movement in the leftward direction. The later parameter similarly indicates the movement of the reference point in up/down directions since the last frame.

The scale, differential scale, and rotation states of the object can be similarly analyzed and represented by parameters output from the gestural decoding module.

Scale state can be discerned by reference to two (or more) reference points on the object (e.g., diagonal corners of a card). The distance between the two points (or the area circumscribed by three or more points) is discerned, and expressed as a percentage of the diagonal size of the image frame (or its area). A single output parameter, A, which may be a seven-bit binary representation, is output.

As with X-Y data, the gestural decoding module can likewise monitor changes in the scale state parameter since the last frame, and product a corresponding output parameter A'. This parameter can be expressed in two's complement form, with positive values indicating movement of the object towards the sensor since the last frame, and negative values indicating movement away.

A differential scale parameter, B, can be discerned by reference to four reference points on the object (e.g., center points on the four edges of a card). The two points on the side edges of the card define a horizontal line; the two points on the top and bottom edges of the card define a vertical line. The ratio of the two line lengths is a measure of differential scale. This ratio can be expressed as the shorter line's length as a percentage of the longer line's length (i.e., the ratio is always between zero and one). Again, a two's complement seven-bit representation can be used, with positive values indicating that the vertical line is shorter, and negative values indicating that the horizontal line is shorter. (As before, a dynamic parameter B' can also be discerned to express the change in the differential scale parameter B since the last frame, again in two's complement, seven bit form.)

A rotation state parameter C can be discerned by the angular orientation of a line defined by two reference points on the object (e.g., center points on the two side edges of a card). This parameter can be encoded as a seven-bit binary value representing the percentage of rotational offset in a clockwise direction from a reference orientation (e.g., horizontal). (The two reference points must be distinguishable from each other regardless of angular position of the object, if data in the full range of 0-360 degrees is to be represented. If these two points are not distinguishable, it may only be possible to represent data in the range of 0-180 degrees.) As before, a dynamic parameter C' can also be discerned to express the change in the rotation state parameter C since the last frame. This parameter can be in seven bit, two's complement form, with positive values indicating change in a clockwise rotation

The foregoing analysis techniques, and representation metrics, are of course illustrative only. The artisan will recognize many other arrangements that can meet the needs of the particular Bedoop applications being served.

In the illustrative system, the Bedoop application programs communicate with the gestural decoding module through a standardized set of interface protocols, such as APIs. One API can query the gestural input module for some or all of the current position parameters (e.g., any or all of X, Y, A, B, and C). The module responds to the calling application with the requested parameter(s). Another API can query the gestural input module for some or all of the current movement data (e.g., any or all of X', Y', A', B' and C'). Still another API can request the gestural decoding module to provide updated values for some or all of the position or movement data on a running basis, as soon as they are discerned from each frame. A complementary API discontinues the foregoing operation. By such arrangement, all of the gestural data is available, but the Bedoop application programs only obtain the particular data they need, and only when they ask for it.

In Bedoop applications that communicate with external servers, just the Bedoop data (i.e., CLASS, DNS, and optionally UID) may initially be sent. If the remote server needs to consider gestural data in deciding how to respond, the remote server can poll the local Bedoop system for the necessary data. The requested gestural data is then sent by the local Bedoop system to the remote server in one or more separate transmissions.

In other embodiments, since the gestural data is of such low bandwidth (e.g., roughly 56 bits per image frame), it may routinely and automatically be sent to the remote computer, so that the gesture data is immediately available in case it is needed. In an illustrative implementation, this data is assembled into an 8-byte packet, with the first byte of the packet (e.g., the X parameter) being prefixed with a "1" sync bit, and subsequent bytes of the packet being prefixed with "0" sync bits. (The sync bits can be used to aid in accurate packet decoding.)

In some embodiments, it is useful to provide for an extension to the normal 64-bit Bedoop length to accommodate an associated packet of gestural data. This can be effected by use of a reserved bit, e.g., in the UID field of the Bedoop packet. This bit normally has a "0" value. If it has a "1" value, that indicates that the Bedoop data isn't just the usual 64 bits, but instead is 128 bits, with the latter 64 bits comprising a packet of gestural data.

Similar extension protocols can be used to associate other ancillary data with Bedoop data. A different reserved bit in the UID field, for example, may signal that a further data field of 256 bits follows the Bedoop data—a data field that will be interpreted by the remote computer that ultimately services the Bedoop data in a known manner. (Such bits may convey, e.g., profile data, credit card data, etc.) The appended data field, in turn, may include one or more bits signaling the presence of still further appended data

Grandmothers

It is a common complaint that computers are too complex for most people. Attempts to simplify computer-user interaction to facilitate use by less experienced users usually serve to frustrate more experienced users.

In accordance with another embodiment of the present invention, the sophistication of a computer user is steganographically indicated on a talisman used by that user to interact with the system. The computer detects this steganographically-encoded data, and alters its mode of interacting with the user accordingly.

Consider internet browser software. Experienced users are familiar with the different functionality that can be accessed, e.g., by various drop-down menus/sub-menus, by the keyboard shortcuts, by the menus available via right-clicking on the mouse, by manipulating the roller mouse scroll wheel and scroll button, etc., etc. Grandmothers of such users, typically, are not so familiar.

Although gestural interfaces hold great promise for simplifying user-computer interaction, the same dichotomy between experienced users and inexperienced users is likely to persist, frustrating one class of user or the other.

To help close this gap, a computer system according to this embodiment of the invention responds to gestures in different manners, depending on the expertise level indicated by encoding of the talisman. For an expert user, for example, the gestural interface active in the internet browser software may display the stored list of Favorite web addresses in response to tipping the left edge of the talisman towards the optical sensor. Once this list is displayed, the expert user may rotate the talisman to the right to cause the highlighting to scroll down the list from the top. Rotating the talisman to the left may scroll the list of Favorites up from the bottom. The speed of scrolling can be varied in accordance with the degree of rotation of the talisman from a default orientation.

In contrast, for the novice user, these talisman manipulations may be confounding rather than empowering. Tipping the left edge of the talisman towards the sensor may occur as often by mistake as on purpose. For such users, a more satisfactory interface may be provided by relying on simple X-Y movement of the talisman to move an on-screen cursor, with a movement of the talisman towards the sensor to serve as a selection signal (i.e., like a left-mouse click).

(In the example just-cited, the expert user summoned a list of Favorite web sites. Different "Favorites" lists can be maintained by the computer—each in association with different talismans. A husband who uses one talisman is provided a different "Favorites" list than a wife who uses a different talisman.)

Printed Pictures

In accordance with this aspect of the invention, a printed photograph can be steganographically encoded with Bedoop data leading to information relating to the depicted person (e.g., contact information, biographical information, etc.).

Such a photograph can be presented to a Bedoop sensor on a telephone. In a simple embodiment, the telephone simply processes the Bedoop data to obtain a corresponding default telephone number, and dials the number. In other embodiments, various options are possible, e.g., dial home number or dial work number. On presenting the photograph to the telephone, for example, moving the photo to the left may dial the person at home, while moving he photo to the right may dial the person at work.

As telephones evolve into more capable, multi-function devices, other manipulations can invoke other actions. In a computer/telephone hybrid device, for example, rotating the photo counterclockwise may launch a web browser to an address at which video data from a web cam at the pictured person's home is presented. Rotating the photo clockwise may present an e-mail form, pre-addressed to the e-mail address of the depicted person. Moving the photo to the right may query a database on the system for other photographs depicting the same individual or subject, which can be presented in response to further user input. Etc.

In this and other embodiments, it is helpful for the Bedoop device to prompt the user to aid in manipulating the object. This can be done audibly (e.g., "move photo left to dial at home") or by visual clues (e.g., presenting left- or right-pointing arrows).

Bedoop data in photographs can also be used to annotate the photographs, as with notes on the back of a photograph, or printed under the photograph in a photo album. The Bedoop data can lead to a remote database, where the photograph owner is permitted to enter a textual (or audio) narrative in association with each photograph's UID. Years later, when some of the names have been forgotten, the photograph can be positioned in front of a Bedoop sensor, and the system responds by providing the annotation provided by the photograph owner years earlier.

Drivers Licenses and Other Cards

Drivers licenses, social security cards, or other identity documents may be encoded by the issuing authority with Bedoop data that permits access to the holder's personal records over the web. On presenting the document to a Bedoop system, the system directs a web browser to a private address corresponding to data encoded on the document. At that address, the holder of the document can review governmental records, such as state or federal tax return data, social security entitlements, etc., as well as privately-maintained records, such as credit records, etc. User selection among various functions can be effected by spatial manipulation of the document. (Entry of additional data, such as social security number or mother's maiden name, may be required of the user to assure privacy in case the document is lost or stolen.)

By manipulating a driver's license in front of a Bedoop sensor, a user can request renewal of the driver's license, and authorize payment of the corresponding fee.

Bank cards (debit, credit, etc.) can similarly be encoded with Bedoop data to permit the holder to access bank records corresponding to the bank card account. (Entry of a PIN code may be required to assure privacy.)

Such documents can also be used to access other personal data. One example is e-mail. A traveler might pause at a Bedoop kiosk at an airport and present a driver's license. Without anything more, the kiosk may present email that is waiting for the traveler on an associated display screen.

On recognizing a driver's license, the kiosk can access a remote site (which may be maintained by the Department of Motor vehicles, another government entity, a private entity, or by the traveler), authenticating the operation by presenting Bedoop data encoded on the license, and obtaining information that the person has pre-approved for release in response to such authorized access. This information can include e-mail account and password information. Using this information, the kiosk queries the corresponding e-mail server, and downloads a copy of recently received mail for presentation at the kiosk. (A user-entered PIN number may be required at some point in the process, e.g., in querying the remote site for sensitive e-mail password data, before presenting the downloaded e-mail for viewing, etc., to ensure privacy.)

Other cards carried in wallets and purses can also be encoded to enable various functions. The local sandwich

shop that rewards regular customers by awarding a free sandwich after a dozen have been purchased can encode their frequent-buyer card with Bedoop data leading to the shop's web-based sandwich delivery service. Or the frequent-buyer card can be eliminated, and customers can instead wave their business card or other identity document in front of the shop's Bedoop sensor to get purchase credit in a tally maintained by the sandwich shop's computer.

Food stamps, health insurance cards, and written medical prescriptions, can likewise be encoded with digital data to enable the provision of new functionality.

At large trade shows, such as COMDEX, vendors needn't publish thick, glossy brochures to hand out to visitors. Instead, they may print various stylish promo cards for distribution. When later presented to a Bedoop sensor, each card leads to a web-based presentation—optionally including persuasive video and other multi-media components. The user can be prompted to provide data to customize, or focus, the presentation to the user's particular requirements. If the user wants further information, a request can be made by the click of a mouse (or the twist of a card).

Prizes and Product Promotions

Product packaging (e.g., Coke cans, Snapple bottles, Pepsi 12-pack boxes) can be encoded for contest purposes. The encoding can be customized, item to item, so that selected items—when Bedoop scanned—are recognized to be the one in a hundred that entitles the owner to a cash or merchandise prize. A remote server to which the item's Bedoop data is provided queries the user for contact information (e.g., address, phone number) so the prize can be awarded or, for smaller prizes, the system can print out an award certificate redeemable at local merchants for products or cash. Once a winning item is identified to the remote server, its UID on the server is marked as redeemed so that the item cannot later be presented to win another prize.

In other such embodiments, all of the items are encoded identically. Winners are determined randomly. For example, during a contest period, persons around the world may present Coke cans to Bedoop systems. The corresponding Bedoop application on each user computer submits Bedoop data to a corresponding web address. The user's e-mail address may also be included with the submission. As this data is relayed to the corresponding server computer(s), every N^{th} set of data is deemed to be a winner, and a corresponding award notification or prize is dispatched to the Bedoop system from which the winning set of data originated.

The server computer that receives such contest submittals from client Bedoop systems can be arranged to prevent a single user from bombarding the server with multiple sets of data in an attempt to win by brute force. (This may be done, for example, by checking the included e-mail address, and not considering a data submittal if the same e-mail address was encountered in data submitted within the past hour. Similar anti-brute-force protection can be provided on the user's computer, preventing, e.g., repeated contest data to be sent more frequently than once per hour. More sophisticated anti-brute-force measures can of course be provided.)

Product Information and Ordering

In accordance with another embodiment of the present invention, product packaging and product advertisements can be encoded with Bedoop data that, when presented to a Bedoop system, initiates a link to a web page from which that product can be purchased, or more information obtained. Once the link has been established, the user can be instructed to manipulate the object in different of the earlier-described modes to effect different functions, e.g., move towards camera to order the product; move away from camera for product information. If the object is moved towards the camera to effect an order, the user can be prompted to further manipulate the object to specify delivery options (e.g., rotate left for overnight mail, rotate right for regular mail). If the object is moved away from the camera to request product information, the user can be promoted to further manipulate the object to specify the type of information desired (e.g., rotate left for recipes, rotate right for FDA nutritional information, move up for information on other products in this family, move down to send an email to the product manufacturer).

Credit card or other customer billing information, together with mailing address information, can be stored in a profile on the Bedoop system, and relayed to the transactional web site either automatically when a purchase action is invoked, or after the user affirms that such information should be sent (which affirmation may be signaled by manipulation of the packaging or advertisement in one of the earlier-described modes). Other modes of payment can naturally be employed. (One such alternative is the first-to-redeem electronic money system described in the present assignee's patent application 60/134,782.)

Clothing

In accordance with another aspect of the invention, clothing can be ordered on-line by presenting to a Bedoop system a photograph from a catalog, or a garment tag or label. Encoded on each is product-identifying data, including a manufacturer ID. The Bedoop system responds by establishing a link to a remote computer maintained by or on behalf of the manufacturer. In addition to relaying the product identification data to the remote computer, the Bedoop application also sends some or all of a clothing profile maintained by the user on the local computer. This profile can specify, e.g., the person's weight, height, shoe size, waist size, inseam, etc. The remote computer can confirm availability of the identified item in the size specified in the clothing profile, and solicit payment and shipping instructions.

Computer Access Cards

This disclosure earlier considered access cards used to gain access to secure buildings. Related principles can be used in conjunction with computer access.

A driver's license, employee photo ID, or other such document can be presented to a Bedoop sensor on a computer. The computer recognizes the user and can take various steps in response.

One response is to log onto a network. Another is to set load a user profile file by which the computer knows how to arrange the desktop in the user's preferred manner. By manipulating the Bedoop-encoded object, the user can further vary the environment (e.g., rotate left to launch standard business productivity applications and software development applications; rotate left to launch lunchtime diversions—stock update, recreational games, etc.).

Hotel rooms are increasingly providing computer services. By presenting a driver's license, a Bedoop-equipped computer in a hotel room can link to a remote site indicated by the Bedoop data, obtain preference data for that user, and launch applications on the hotel computer in an arrangement that mimics that user's familiar work computer environment.

Audio/Video Disks, Software, and Books

Bedoop data can be conveyed by indicia or texturing on the surfaces of CD and DVD disks, on the labels (or authenticity certificates) for same, on the enclosures for same (e.g., jewel box, plastic case, etc.), on book dust

jackets, on book pages, etc. Any of these objects can be presented to a Bedoop device to establish a link to a related web site. The consumer can then manipulate the object (or otherwise choose) to select different options.

For music, one option is to receive MP3 or other clips of songs by the same artist on other CDs, or of songs from other artists of the same genre. Another is to view music video clips featuring the same artist. Still another is to order tickets to upcoming concerts by that artist. In-store kiosks can permit tentative customers to listen to sample tracks before they buy.

Similar options can be presented for video DVDs. In the case of video, this can include listings of other movies with the same director, with the same star(s), etc. In the case of software, the options can include advisories, bug fixes, product updates and upgrades, etc. Naturally, the user can make purchases from these sites, e.g., of other music by the same artist, other videos with the same star, software upgrades, etc.

Similar options can be accessed using Bedoop data associated with printed book materials.

Ad Tracking

Advertisers commonly use different advertisements for the same product or service, and employ means to track which ad is more effective within which demographic group. Bedoop can provide such functionality.

Consider a travel service web site that is promoting Hawaiian vacations. Bedoop data from several advertisements can lead consumers to the site.

Identical advertisements can be placed in several different magazines. Each is encoded with a different Bedoop UID. By monitoring the UIDs of the Bedoop inquiries to the site, the travel service can determine which magazines yield the highest consumer response (e.g., per thousand readers).

Likewise, within a single magazine, two or more advertisements may be encoded with Bedoop data leading to the site—again, each with a different UID. Again, analysis of the UIDs used in accessing the site can indicate which advertisement was the more effective.

The instantaneous nature of the internet links permits advertisers to learn how consumer responses to print advertisements vary with time-of-day, yielding information that may assist in making ads for certain products more effective.

More elaborate variants and combinations of the foregoing are, of course, possible, If the consumers provide personal information in response to the ads (either by permitting access to pre-stored personal profile data, or by filling in web-based forms, or by manipulation of the ad (e.g., "please move the ad towards your Bedoop sensor if you drank coffee this morning")), still richer statistical data can be gleaned.

Rolodex of Cards

Bedoop-encoded business cards as detailed above can be accumulated and kept near a telephone or computer in a Rolodex-like arrangement. If a refrigerator ice-maker malfunctions, a homeowner can find the card for the appliance repairman used a few years ago, and present it to a Bedoop sensor. A link is established to the repairman's company (e.g., web site or via telephone). At a web site, the repairman may provide basic information, such as hours of availability, current fee schedule, etc. The homeowner may select an option (by card gesture or otherwise) to invoke a teleconference (e.g., NetMeeting) to consult about the problem. Or the homeowner may select another option to send e-mail. Still a further option may permit the homeowner to schedule a house call on the repairman's weekly calendar. Still a further option may permit the homeowner to view one or more short videos instructing customers how to fix certain common appliance problems.

Stored Value Cards

The earlier cited "first-to-redeem" electronic money system may encode Bedoop data on a card that leads to storage at which the random-number tokens (which represent increments of money) are stored. Presenting the card to a Bedoop system launches an application that reads and encrypts the tokens and forwards the encrypted data to the clearinghouse computer of the corresponding bank to learn their remaining value. There the tokens are decrypted and checked for validity (but not redeemed). The bank computer responds to the Bedoop system, indicating the remaining value of the tokens on the card.

For security reasons, the storage containing the random-number tokens should not be generally accessible. Instead, the user must provide authentication data indicating authorization to gain access to that information. This authentication data may be a PIN code. Or the user may provide authentication by presenting a second Bedoop-encoded object, e.g., a driver's license to the Bedoop system. (Many other Bedoop systems may advantageously use, or require the use of, two or more Bedoop objects—either presented one after the other, or all at the same time. The Bedoop system can provide visual or audible prompts leading the user to present the further Bedoop object(s) as necessary.

Ski Lift Tickets

In accordance with another embodiment, ski lift tickets are Bedoop encoded to provide, various functionality.

For example, instead of buying a lift ticket good for a day, a skier may purchase a ticket good for eight lifts. This data is encoded on the ticket, and sensed by a Bedoop sensor at each lift. The sensors are networked to a common server that tracks the number of lifts actually purchased, and updates the number as used. The skier is informed of the number of rides remaining on entering or leaving the lift. Statistical data can be collected about trail usage (e.g., N % percent of skiers ski all day along just two lifts, etc.).

Off the slopes, back at home, the used lift ticket may be presented to a Bedoop sensor to obtain current snow conditions and lift hours, or to review trail maps, or to order ski vacation packages. If the ticket is encoded with the owner's name, UID, or other information of commercial/marketing interest, local merchants may give the bearer discounts on selected goods in response to Bedoop scanning of the ticket and recovery of such information.

REI Membership Cards

Membership cards for certain stores can be Bedoop-encoded to provide added value to the member. For outdoor gear stores such as REI, presentation of the card to a Bedoop sensor can lead to a library of USGS maps, to web pages with current fishing and hunting regulations, etc. Naturally, the store's on-line ordering site is just a quick twist away.

Theme Park Tickets

Theme park tickets can be encoded with the age and gender of the visitor, and with additional data permitting the experience to be customized (e.g., from a roster of theme park personalities, the visitor's favorite is Indiana Jones). Throughout the park are kiosks to which the visitor can present the ticket to orchestrate the visit to follow a particular story line. Some kiosks issue premiums matching the age/gender of the recipient.

Car Keys

In accordance with another embodiment of the invention, car keys (or key ring fobs) are Bedoop encoded. When the car is taken to a shop for service, the mechanic presents the key to a Bedoop sensor, and thereby obtains the car's

maintenance history from a remote server on which it is maintained. At home, the key can be presented to a Bedoop sensor and manipulated to navigate through a variety of automotive-related web sites.

In some embodiments, the Bedoop-encoded object is not used to navigate to a site, but is instead used to provide data once a user's computer is otherwise linked to a web site. A user surfing the web who ends up at a car valuation site can present a key to the Bedoop scanner. The Bedoop data is used to access a remote database where the make, model, options, etc., of the car are stored. This data is provided to a database engine that returns to the user the estimated value of the car.

While visiting a mechanic's web site, presentation (and optionally manipulation) of a key or key ring fob can be employed to schedule a service appointment for the car.

Fashion Coordination

Some department stores and clothing retailers offer "personal shoppers" to perform various services. For example, a customer who is purchasing a dress may ask a personal shopper for assistance in selecting shoes or accessories that complement the dress.

A Bedoop-encoded garment tag on the dress can be employed to obtain similar assistance. In response to such a tag, a Bedoop system can query a database to obtain a mini-catalog of clothes and accessories that have previously been identified as complementing the dress identified by the tag. These items can be individually displayed on a screen associated with the system, or a virtual model wearing the dress—together with one or more of the recommended accessories—can be synthesized and depicted. The shopper may quickly review the look achieved by the model wearing the dress with various different pairs of shoes, etc., by repeatedly activating a user interface control (by mouse, touch screen, or garment tag gestures) to cycle through different combinations.

A shopper's credit card can be Bedoop-encoded so as to lead Bedoop systems of particular stores (i.e., stores pre-authorized by the shopper) to a profile on the shopper (e.g., containing size information, repeat purchase information, return history, style/color preferences, etc.).

Credit Card Purchases

When a consumer visits a commercial web site and wishes to purchase a displayed product, the transaction can be speeded simply by presenting a Bedoop-encoded credit card to a Bedoop sensor on the user's computer. The Bedoop data on the card leads to a database entry containing the credit card number and expiration date. The Bedoop application then sends this information (optionally after encrypting same) to the web site with instructions to purchase the depicted product.

(Impulse purchases are commonly deterred by the hurdles posed between the purchase impulse and the completed purchase. This and other Bedoop applications aid in reducing such hurdles.)

Product Marketing

Bedoop data relating to one product or service can be used to cross-market others products and services. Consider a consumer who purchases a pair of golf shoes. The box is Bedoop encoded. By presenting the box to a Bedoop system, the consumer is linked to a web page that presents various promotional offers. The consumer may, for example, elect to play a free round of golf at one or more identified local golf courses, or print a coupon for ten percent off any order of socks from an on-line sock merchant. (Various means can be employed to prevent multiple redemptions from a single box. One is a serial number that is tracked by the web page or cross-marketed merchant, and only honored once. Another is identification data corresponding to the consumer that is tracked to prevent multiple redemptions.)

Product tags can likewise be Bedoop-encoded. A tag from an article of Nike apparel can lead to the Nike on-line store, where the user can buy more merchandise. If the tag is from a soccer jersey, a certain tag manipulation (e.g., rotate left) may lead the user to a special-interest soccer page, such as for the World Cup. A tag on a golf glove may lead to a website of a local golf course. Twist left to reserve a tee time; twist right to review course maps and statistics. Bedoop kiosks can be provided in retail stores to let consumers use the Bedoop features.

Travel Planning Services

After making a reservation at a resort, a consumer is typically mailed (by email or conventional mail) various confirmation information. If not already printed, the consumer can print this information (e.g., a confirmation card).

Bedoop-encoding on the printed object can lead to web-based information relating to the reservation (e.g., reservation number, the consumer's name, arrival/departure dates, etc.). If the consumer wishes to make dinner or golf reservations, this object is presented to a Bedoop system—either at the user's home, at an airport kiosk, etc. The system recognizes the object type and encoded data, and establishes a link to a remote computer that provides various information and scheduling services for the resort. By manipulating the object (or otherwise) the consumer selects desired dinner and golf tee times. The system already has the reservation number (indexed by the UID), so tedious provision of such data is avoided.

In some embodiments, the remote computer is not maintained by the resort, but is rather maintained by an independent travel service. (The travel service may also maintain the DNS leaf node server.) The computer can present a web page (branded by the travel service or not) that offers the scheduling options desired by the user, and also presents links to other information and services (e.g., offering entry tickets to nearby attractions, and advertising nearby restaurants).

Airline tickets (or e-ticket confirmations) can be similarly encoded with Bedoop data. These items may be presented to Bedoop systems—at a traveler's home or in airports—to permit review and changing of travel itinerary, reserve hotels and rental cars, secure first-class upgrades, check the airplane's seating arrangement, review frequent flier status, scan tourist information for the destination, etc.

Movie Tickets

As indicated earlier, movie tickets can be encoded with Bedoop data identifying, e.g., the movie title and date. When a movie viewer returns home, the ticket stub can be presented to a Bedoop system. One of the options presented by the corresponding Bedoop application can be to launch a pay-per-view screening of the just-seen movie at a discounted rate. Another is to download the movie onto a writeable DVD disk at the viewer's home, perhaps serialized to permit playback only on that viewer's DVD player, or enabled for only a few playbacks, etc. (again, likely for a discounted fee). Still another option is to present web-delivered video clips from the movie. Another is to offer related merchandise for purchase, possibly at discount to retail. (These features may be available for only a limited period after the date encoded on the ticket stub.) Another is to alert the consumer to upcoming movies of the same genres, or with the same director or stars, or released by the same studio. Still another is to direct a web browser to an on-line ticket merchant for tickets to other movies. The consumer may navigate among these options by manipulating the ticket stub, or otherwise.

The same, or related, options can likewise be provided in response to Bedoop data detected from a book jacket presented to a Bedoop system.

Video Recording

A video recording device can be programmed to record a broadcast program by presenting a Bedoop sensor with a printed promotion for the program (e.g., an advertisement in a newspaper or TV Guide). Bedoop-encoded within the printed document is data by which the Bedoop system (which may be built into the video recorder or separate) can set the recording time, date, and channel.

Set Top Boxes

Many entertainment-related applications of Bedoop data can be implemented using television set top boxes. Such boxes include processors, and typically include a return channel to a control facility. The provision of a Bedoop chip and optical sensor can vastly increase the functionality these devices presently provide.

Special Event Tickets

Consider a ticket to a basketball game. By presenting the ticket to a Bedoop system, a user may access the web site of either team so as to review recent scores and statistics. The user may also obtain a web-based virtual tour of the arena, and review seating maps. Tickets for upcoming games may be ordered, as well as pay-per-view games and team souvenirs. For high-priced tickets, the user may be entitled to premium web features, such as on-line text-, audio-, or video-chat session with a team star on the day before the game.

Unlike conventional tickets, Bedoop-encoded tickets need not limit the user to a predetermined seat. While the ticket may be printed with a nominal seat, the user may present the ticket to a Bedoop sensor and access a web site at which a different seat can be reserved. On attending the event, the consumer presents the ticket to a Bedoop sensor that reads the ticket UID and looks up the seat assignment most-recently picked by the consumer. It then prints a chit entitling the consumer to take the seat earlier selected from the transactional web site.

Signet Rings

Signet rings have historically been used to indicate a person's identity or office. Such rings, or other items of personal jewelry, can be encoded with Bedoop data (either by texturing or printing) and presented as necessary to Bedoop systems. The extracted Bedoop data can lead to a secure web site indicating the person's name and other information (i.e., a web site that has anti-hacking measures to prevent illicit change of the stored identification information). Such a signet ring can be presented to Bedoop systems that require a high-confidence confirmation of identity/authorization before proceeding with a Bedoop function.

Post-It® Notes

Pads of Post-It® notes, or other pads of paper, can be marked by the manufacturer (either by texturing, water-marked tinting, ink-jet spattering, etc.) to convey steganographic data (e.g., Bedoop data). When such a note is presented to a Bedoop system, the system may launch an application that stores a snapshot of the note. More particularly, the application may mask the note-portion of the image data from the other image data, virtually re-map it to a rectangular format of standardized pixel dimensions, JPEG-compress the resulting image, and store it in a particular computer subdirectory with a name indicating the date of image acquisition, together with the color and/or size of the note. (These latter two data may be indicated by data included in the Bedoop payload.) If the color of the note is indicated by digital data (e.g., in the file name), then the image itself may be stored in grey-scale. When later recalled for display, the white image background can be flooded with color in accordance with the digital color data.

The Bedoop system may buffer several past frames of image data. When the object is recognized as a Post-It note whose image is to be saved, the system may analyze several such frames to identify the one best-suited for storage (e.g., check the spatial frequency content of the note as imaged in each frame, to identify the one with the finest detail), and store that one.

When a Post-It note is recognized by the Bedoop system, the system may emit a confirmation tone (or other response) to indicate that the object has been recognized, but not immediately execute the snapshot operation. Instead, the system may await a further instruction (e.g., gesture) to indicate what operation is desired.

By moving the note towards the sensor, for example, the user can signal that a snapshot operation is to be performed. (This closer presentation of the note may also permit the imaging system to capture a more detailed frame of image data.)

By moving the note away, the system may respond by reading, decompressing, and displaying the six most-recently stored Post-It note images, in tiled fashion, on the computer screen. The individual notes can be displayed at their original dimensions, or each can be re-sized to fill the full height or width of a tile. A user interface control (responsive to gestures, mouse operation, keyboard scroll arrows, etc.) allows the user to scroll back in time to any desired date.

The full 64-bit Bedoop payload of other embodiments may not be needed for Post-It notes. In the just-given example, for example, the Bedoop system responds to all Post-It notes in the same fashion. Thus, an abbreviated Bedoop format that indicates simply 'I'm a Post-It note, yellow, size 3"×3"' can suffice. The twelve bit CLASS ID, with eight further bits to indicate color/size combinations, may be sufficient. Reducing the payload permits it to be more robustly encoded on small objects. (As noted below, Bedoop decoding systems can look for several different data formats/protocols in trying to extract Bedoop data from an object.)

Alignment of Documents for Other Purposes

While the just-described pre-marked paper triggered a Bedoop response when presented to a Bedoop sensor (i.e., take a snapshot of the paper), the markings can be used for purposes other than to trigger Bedoop responses. Regardless of the particular data with which the paper is encoded, the embedded subliminal graticules, or other steganographically-encoded registration data, can be used by other applications to correct misalignment of scanned data. In a photocopier, for example, a document need not be placed exactly squarely on the glass platen in order to yield a properly-aligned photocopy. The scanner scans the skewed document and then detects the steganographic registration markings in the resulting scan data. This data is then processed to virtually re-register same, so that the registration markings are in a desired alignment. The processed scan data is then provided to the xerographic reproduction unit to yield a photocopy in which the skew effect is removed.

The same technique is likewise applicable to video recorders, digital cameras, etc. If such a device images an object (e.g., a photograph) with steganographic registration markings, these markings can be used as a guide in re-registering the resulting data to remove mis-alignment effects.

Postal Mail Information

Many contexts arise in which data to be presented to a consumer is valuable only if timely. The postal service mail is ill-suited for some such information due to the latency between printing a document, and its ultimate delivery to a recipient. Bedoop principles, however, allow the recipient to take a postal object that was printed well before delivery, and use it on receipt (i.e., present to a Bedoop system) to receive up-to-the-minute information. In this and other embodiments, the Bedoop data can also uniquely identify the addressee/recipient/user, so the web site can present data customized to that user.

Distributors of printed advertising can reward Bedoop-driven consumer visits to their web sites by issuing digital tokens or coupons that can be redeemed for premiums, cash-back, etc. Every millionth visitor wins a million pennies (with appropriate safeguards, e.g., preventing more than one entry an hour).

Classes of Bedoop Encoding

The above-described embodiments focused on use of Bedoop data after decoding. Additional insight may be gained by examining the earlier part of the process—encoding.

Encoding can be performed in many contexts, which may be conceptualized as falling into three broad classes. The first is static marking, in which a document designer, pre-press service bureau, advertising agency or the like embeds Bedoop data. The second is dynamic marking, in which automated systems encode, or vary, Bedoop data "on the fly." Such systems can tailor the Bedoop data to particularly suit the context, e.g., to the moment, place, user, etc. The third is consumer marking, in which Bedoop data is added to a document at the time of printing.

The second class of encoding enables features not available from the first. Consider an American Express travel web page with information about travel to Hawaii. A DNS leaf node server points to this page in response to certain Bedoop data—e.g., data encoded in a magazine photograph of a Hawaiian beach scene.

Actually, all Bedoop data having a certain CLASS and DNS ID may lead to this web page, irrespective of the UID data. If the magazine photo is encoded with a particular "don't care" UID field(e.g., 11111111111111111111), this may signal the originating Bedoop system—or any intervening system through which the Bedoop data passes—that arbitrary data can be inserted in the UID field of that Bedoop packet. The originating Bedoop system, for example, can insert a dynamically-configured series of bits into this field. Some of these bits can provide a profile of the user to the remote server, so that the Bedoop response can be customized to the user. (The user would naturally pre-approve information for such use so as to allay privacy concerns.)

As one example, the local Bedoop system can set the least significant bit of the UID field to a "0" if the user is male, or to a "1" if the user is female. The next four bits can indicate the user's age by one of sixteen age ranges (e.g., 3 or less, 4-5, 6-7, 8-9, 10-11, 12-13, 14-15, 16-17, 18-20, 21-24, etc.).

Alternatively, or in addition, the local Bedoop system can stuff the don't-care UID field (all of it, or in part) with signature data tending to uniquely identify the local Bedoop system (e.g., system serial number, a hash code based on unchanging data unique to that system, etc.) By reference to such data, the remote server can identify repeat visits by the same user, and can tailor its responses accordingly (e.g., by recalling a profile of information earlier entered by the user and stored at the remote server, avoiding the need for data re-entry).

More on Optical Input Devices

It is expected that image input devices will soon become commonplace. The provision of digital cameras as built-in components of certain computers (e.g., the Sony Vaio laptops) is just one manifestation of this trend. Another is camera-on-a-chip systems, as typified by U.S. Pat. No. 5,841,126 and detailed in Nixon et al., "256×256 CMOS Active Pixel Sensor Camera-on-a-Chip," IEEE J. Solid-State Circuits, Vol. 31(12), pp. 2046–2051 (1996), and Fossum, "CMOS Image Sensors: Electronic Camera-on-a-Chip," IEEE Transactions of Electron Devices, vol. 44, No. 10, October 1997. Still another is head-mounted cameras (as are presently used in some computer-augmented vision systems). These and other image input devices are all suitable for use in Bedoop systems.

Camera-on-a-chip systems can be equipped with Bedoop detector hardware integrated on the same chip substrate. This hardware can be arranged to find and decode Bedoop data from the image data—notwithstanding scale, rotation, differential scaling, etc. Gestural decoding can also be provided in hardware, with the resulting data output in packet form on a serial output bus. Such a chip can thus provide several outputs—image data (either in raw pixel form, or in a data stream representing the image in one of various image formats), 64 bits of Bedoop data (serially or in parallel), and decoded gesture data.

In other embodiments, the Bedoop detector (and/or the gestural decoder) can be on a substrate separate from the camera system.

To accommodate different Bedoop data formats and protocols, the hardware can include RAM or ROM in which different format/protocol information is stored. (These different formats/protocols can relate, e.g., to Bedoop systems employing different data payload lengths, different sublimінal grids, different encoding techniques, etc.) As the Bedoop system stares out and grabs/analyzes frames, each frame can be analyzed in accordance with several different formats/protocols to try and find a format/protocol that yields valid Bedoop output data.

Movable Bedoop Sensors

Although the illustrated Bedoop systems are generally stationary, they need not be so. They can be portable. Some such systems, for example, employ palmtop computers equipped with optical sensor arrays. If the palmtop is provided with live network connectivity (e.g., by wireless), then Bedoop applications that rely on remote computers can be implemented just as described. If the palmtop is not equipped with live network connectivity, any Bedoop applications that rely on remote computers can simply queue such communications, and dispatch same when the palmtop next has remote access (e.g., when the palmtop is next placed in its recharger and is coupled to a modem through which internet access can be established).

Another variant is a Bedoop sensor that is movable around a desk or other work-surface, like a mouse. Such a sensor can be coupled to the associated computer by cabling, or a wireless interface can be used. The peripheral may be arranged for placement on top of an item in order to read digital data with which the object is marked. (Built-in illumination may be needed, since the device would likely shadow the encoding.) Some forms of such peripherals are adapted to serve both as general purpose digital cameras, and also as Bedoop sensors.

Such a peripheral would find many applications. In "reading" a magazine or book, for example, it may be more intuitive to place a Bedoop reader "on" the object being read, rather than holding the object in the air, in front of a

Bedoop sensor. This is particularly useful, e.g., when a magazine page or the like may have several differently-encoded Bedoop sections (corresponding to different articles, advertisements, etc.), and the user wants to assure that the desired Bedoop-encoded section is read.

The "bookmark" paradigm of internet browsers might be supplemented with paper bookmarks, e.g., Bedoop data encoded on one or more pages of paper. To direct a browser to a particular bookmarked destination, the peripheral is simply placed on top of the page (or part thereof) that is marked with the corresponding Bedoop data. A user may print a "Map" comprised of postage stamp-sized regions tiled together, each of which regions represents a favorite web destination.

Such a map may be printed on a mouse pad. Indeed, mouse pads with certain maps pre-encoded thereon may be suitable as promotional materials. A company may offer to print a family photograph on such a pad. Encoded within the photograph or the pad texture are addresses of web sites that have paid a fee to be accessible in this manner on a user's desk.

Like mice—which are provided with buttons, roller wheels, and roller buttons in addition to X-Y encoders—movable Bedoop encoders can likewise be provided with auxiliary switches and roller inputs to complement the data input provided by the optical sensor. Indeed, some embodiments integrate the functions of Bedoop peripheral with a mouse. (The undersides of mice are generally under-utilized, and can readily be equipped with an image sensor.) Gestural input can readily be provided by such a peripheral—in this context moving the sensor rather than the object.

Watermarking Techniques

There are nearly as many techniques for digital watermarking (steganographic data encoding) as there are applications for it. The reader is presumed to be familiar with the great variety of methods. A few are reviewed below.

The present assignee's prior application Ser. No. 09/127,502, filed Jul. 31, 1998, shows techniques by which very fine lines can be printed on a medium to slightly change the medium's apparent tint, while also conveying digital data. Commonly-owned application Ser. No. 09/074,034, filed May 6, 1998, details how the contours of printed imagery can be adjusted to convey digital data. (That technique can be applied to printed text characters, as well as the line art imagery particularly considered.) The assignee's U.S. Pat. No. 5,850,481 details how the surface of paper or other media can be textured to convey optically-detectable binary data. The assignee's U.S. Pat. No. 5,841,886 and 5,809,160 detail various techniques for steganographically encoding photographs and other imagery.

Some watermarking techniques are based on changes made in the spatial domain; others are based on changes made in transformed domains (e.g., DCT, wavelet). Watermarking of printed text can be achieved by slight variations to character shape, character kerning, line spacing, etc.

Data glyph technology, as detailed in various patents to Xerox, is usable in many of the applications detailed herein.

The foregoing is just a gross under-sampling of the large number of watermarking techniques. The artisan is presumed to be familiar with such art, all of which is generally suitable for use in the applications detailed herein.

More generally, essentially any data encoding method that permits recovery of the encoded data from optical scan data can be employed. Bar codes (1D and 2D) are but the most familiar of many such optically-detectable data encoding techniques.

Conclusion

Having described and illustrated the principles of our invention with reference to illustrative embodiments, it should be recognized that the invention is not so limited.

For example, while certain of the embodiments were illustrated with reference to internet-based systems, the same techniques are similarly applicable to any other computer-based system. These include non-internet based services such as America Online and Compuserve, dial-up bulletin board systems, etc. Likewise, for internet-based embodiments, the use of web browsers and web pages is not essential; other digital navigation devices and other on-line data repositories can be similarly accessed.

Similarly, while the details of the preferred Bedoop system were particularly given, the underlying principles can be employed in numerous other forms.

For example, one other form is to steganographically encode physical objects with Digital Object Identifiers (DOIs). The Center for National Research Initiatives and the Digital Object Identifier Foundation (www.doi.org) have performed extensive work in establishing an infrastructure by which digital objects can be distributed, tracked, and managed. Some of this same infrastructure and technology can be adapted, in accordance with the teachings provided above, to associate new functionality with physical objects.

Another form is not to reference a remote data repository by data embedded on an object, but instead to encode the ultimate data directly on the object. A photograph, for example, can be literally encoded with a telephone number. On presenting the photograph to an optical sensor on the telephone, the telephone can analyze the optical information to extract the telephone number, and dial the number, without the need for any external data. Similarly, a printed office document (e.g., spreadsheet) can be encoded with the path and file name of the corresponding electronic file, obviating the need for indirect linking (e.g., to a database to correlate a UID to a computer address). Most of the above-described embodiments are suitable for such direct encoding of the related data.

In the business card example given above, the detailed techniques can be supplementary to existing optical character recognition techniques. That is, the image data from an optical sensor can be applied both to a Bedoop decoder and to an OCR system. Text characters discerned by the OCR system can be entered directly into a contacts manager personal database. The techniques employed in the Bedoop system to locate the encoded object and handle visual distortion (e.g., the visual artifacts due to scale, rotation, etc.) can advantageously be used in OCR detection as well, permitting extraction of the OCR information without careful placement of the card.

While certain of the foregoing embodiments made reference to ink-jet printing, similar advantages can often be obtained with other printing technologies, e.g., laser/xerographic printing, offset printing, etc.

In the foregoing embodiments, Bedoop decoding generally proceeded from image data obtained from a physical object. However, in some contexts, it is advantageous to Bedoop-decode image data provided electronically, e.g., over the internet.

Likewise, while the foregoing embodiments generally relied on Bedoop image sensors that stared out for an object at an expected point, in alternative embodiments, sensors that seek rather than stare can be employed (as was illustrated above in connection with the elevator example).

Similarly, while the illustrated embodiments generally employed sensors that repeatedly grabbed frames of image data, this need not be the case. Single frame systems, such

as flatbed scanners, and video systems arranged to grab single frames—with or without TWAIN interfaces—can alternatively be used.

As indicated above, while steganographic encoding of the digital data is used in the preferred embodiments, visible forms of digital encoding—such as bar codes—can naturally be employed where aesthetic considerations permit.

In certain of the embodiments, digital data conveyed by means other than optical can be used. Electromagnetic detection (e.g., of the sort used in proximity-based card-access systems) can be arranged to decode digital data, permitting "at-a-distance" reading of data from physical objects, just as in the foregoing embodiments.

Since the Bedoop image sensors typically acquire plural frames of data, the extraction of the digital data can be based on more than a single image frame. More confidence in the results may be accumulating decoded data over several frames. Moreover, movement of the object within the sensor's field of view may permit the system to acquire information from other perspectives, etc., enhancing system operation.

While the preferred embodiments employ 2-D image sensors (e.g., CCDs), other optical sensing technology can alternatively be employed. Supermarket laser scanners, for example, can read bar-code data. Raster-scanning of such systems can permit acquisition of 2-D data (either in bit-mapped form, or grey-scale).

While the illustrated embodiments used a 12/24/24 bit protocol for CLASS/DNS/UID data, other arrangements can of course be used. In some applications it is advantageous for the protocol to more nearly match those commonly used for internet communications. For example, IP addresses for internet Domain Name Servers (DNS) are presently 32 bits, with extension to 64 or 128 bits foreseen in the near future. The DNS field in Bedoop systems can be follow the internet standard.

Some embodiments can advantageously employ texture-based Bedoop encoding of objects. Bedoop texturing can be effected by various means, including pressure rollers, chemical or laser etching, etc.

While the foregoing embodiments have generally employed planar objects to convey the digital encoding, this need not be the case. Objects of other shapes can likewise be employed. Some shapes present relatively straightforward image processing tasks. Data imaged from a soft drink can or other cylindrical surface, for example, is fairly easy to remap using known geometrical transforms so as to essentially "unwrap" the printing from the can. Other geometries can present more complex re-mappings, but are likewise generally within the capabilities of the artisan. (Such remapping is facilitated by encoding in the data certain reference markings, such as subliminal graticules, etc. The unknown 3D shape of the object being imaged can usually be inferred from the apparent warping of the reference markings in the 2D image data generated by the scanner. Once the warping is characterized, it is generally straightforward to un-warp so as to prepare the image data for decoding.)

It was once popular to predict that paper documents would be replaced with electronic media. In hindsight, electronic media may be recognized as a poor surrogate for paper. Electronic media conveys information flawlessly, but is lacking in experiential attributes. We can hold paper, stack it, own it, deface it, give it, guard it, etc. It provides an opportunity for physical dominion entirely lacking with electronic media.

From the foregoing discussion it can be seen that, rather than replacing paper with electronic media, perhaps the future lies in giving paper digital attributes—hybridizing the physical experience of paper with the technical advantages of digital media. Such an arrangement makes available a great wealth of new functionality, now accessible through familiar paper items, rather than through a "computer input peripheral."

To provide a comprehensive disclosure without unduly lengthening this specification, applicant incorporates by reference the patents, applications, and publications identified above.

In view of the many embodiments to which the principles of my invention may be applied, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of my invention. Rather, I claim as my invention all such embodiments as fall within the scope and spirit of the following claims, and equivalents thereto.

APPENDIX A

PAPER-BASED CONTROL OF COMPUTER SYSTEMS

Related Application Data

This application is a continuation-in-part of co-pending application Ser. No. 09/130,624, filed Aug. 6, 1998, which is a continuation of application Ser. No. 08/508,083 (now U.S. Pat. No. 5,841,978).

The subject matter of this application is generally related to that in all of the assignee's other patents and applications, e.g., U.S. Pat. Nos. 5,841,886, 5,832,119, 5,822,446 and 5,841,978, and the application entitled Methods and Systems Employing Digital Watermarking, filed on even date herewith.

Field of the Invention

The present invention relates to use of printed documents to control computer systems. Exemplary documents include business cards, advertisements, and identification badges, but the invention is not so limited.

Background and Summary of the Invention

Over the past century, business cards have formed part of business ritual. Functionally, they serve as a record of an encounter, and detail means by which the giver may be contacted (address, phone, etc.).

Business cards have changed, essentially, not at all in response to the advent of computers. Some accommodation has been made for business cards on the computer side, in the form of specialized scanner and optical character recognition tools by which textual data printed on cards can be read and entered into personal productivity software tools (e.g. contact managers, address books, datebooks, personal information managers, etc.). However, the data transferred into the personal productivity software is static and unchanging.

In accordance with one embodiment of the present invention, the textual information on a business card is supplemented with steganographically-encoded, multi-bit binary data. This latter data does not significantly distract from the visual aesthetics of the card (as would a bar code or the like), yet can be used by an associated computer to initiate a link to an internet site corresponding to the business card giver. At the site, the recipient of the card may gain access to the giver's schedule, and other information that changes over time. (Such information may not generally be available over the internet to persons without the card data.)

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

FIG. **1** (omitted) shows a flow chart of a process according to one embodiment of the present invention.

Detailed Description

Digital watermarking is a quickly-growing field of endeavor, and many techniques are known. Generally, all seek to steganographically convey multi-bit data ancillary to some other signal or medium.

The present assignee's prior application Ser. No. 09/127,502, filed Jul. 31, 1998, shows techniques by which very fine lines can be printed on a medium to slightly change the medium's apparent tint, while also conveying digital data. Commonly-owned application Ser. No. 09/074,034, filed May 6, 1998, details how the contours of printed imagery can be adjusted to convey digital data. (That technique can be applied to printed text characters, as well as the line art imagery particularly considered.) Applicant's U.S. Pat. No. 5,850,481 details how the surface of paper or other media can be textured to convey optically-detectable binary data. Applicant's U.S. Pat. Nos. 5,841,886, 5,809,160, and the priority applications detailed above, detail various techniques for steganographically encoding photographs and other imagery.

Three papers by Brassil et al show other techniques for conveying watermark data by slight changes to printed text, "Electronic Marking and Identification Techniques to Discourage Document Copying," Proceedings of INFOCOM '94 Conference on Computer, IEEE Comm. Soc Conference, Jun. 12–16, 1994, pp. 1278–1287; "Hiding Information in Document Images," November, 1995, 7 pages, AT&T Bell Laboratories Technical Report (available at ciss95_ps.z from ftp://ftp.research.att.com/dist/brassil/1995/ciss95.ps.Z.; and "Document Marking and Identification using Both Line and Word Shifting," INFOCOM '95 (available at ftp://ftp.research.att.com/dist/brassil/1995 infocom95.ps.Z).

The foregoing is just a sampling of the large literature on watermarking. The artisan is presumed to be familiar with such art, all of which is generally suitable for use with the novel concepts detailed below.

In accordance with any of the known watermarking techniques, a business card is steganographically encoded with plural bit data. At least part of this data identifies an internet address or web site at which data about the giver of the card is stored. If sufficient bits can be encoded into the business card, the address can be encoded literally, e.g., by ASCII or binary numeric encoding. Alternatively, to reduce the data payload, an abbreviated form of address. One example of such an abbreviated form is a Unique Identifier (UID) which can be, e.g., a 24-bit value.

Desirably, the steganographic encoding is tailored to facilitate decoding in the presence of arbitrary rotation or scale distortion of the card introduced during scanning. (Some such techniques are shown, e.g., in applicant's related patents identified above. Others are known to artisans.)

As shown in FIG. **1** (omitted in this appendix), the card is scanned (e.g. by use of conventional opto-electronic devices, such as a scanner or a digital camera). The output data is then optionally processed to account for any skew or scale factor. The plural-bit digital data is then decoded and stored, e.g., in personal productivity software.

(Although not particularly shown in FIG. **1**, it is expected that the detailed process will often be supplemental to known OCR-reading of business cards, and entry of the textual data into personal productivity software. That is, the scan data is processed both by OCR techniques, and by steganographic decoding techniques, and the results of both operations stored in a data structure or other memory for later reference.)

The steganographically-decoded plural-bit data is provided to a web browser or other internet appliance and used to initiate a link to a remote computer over the internet's network of computers. If the remote address was literally encoded in the business card, that address is used directly. If an abbreviated form of address was encoded, an additional step may be required.

If a UID was encoded in the card, rather than a literal address, the web browser might consult an index to correlate the UID to an address. The index could be a table or other data structure stored on the user's local computer, but more commonly is a remote name server database to which the browser links as a default when processing business card UIDs. Data obtained from the index is then used to complete the linking to the ultimate destination. (In addition to reducing the business card payload, such linking through an index, e.g., by a UID, offers flexibility in that the ultimate destination can be moved to other server sites as needed, with just a simple update to the index. Alternatively, all business cards encoded with the former address would be rendered obsolete if the site were relocated.)

At the ultimate site, the user is presented with whatever information the business card giver chooses to provide, including biographical information, photos, promotional offers or advertisements relating to the card-giver's business (or relating to enterprises to whom the card-giver has rented screen space), etc., etc.. In one embodiment, the giver's site is linked to the giver's personal productivity tool(s) and permits viewing, e.g., of calendar information (showing where the business card giver is scheduled to be today, or for the rest of the week, month, etc.).

Typically, this calendar information is not available to casual web browsers; the steganographically decoded data from the business card includes some authentication data (akin to a password) that permits access to otherwise restricted data. This authentication data can take the form of a web page address to which no publicly-accessible link points, a password that is separately presented to the web server by the user's browser after a link is established, or other known technique.

In one form of the invention, the giver of business cards may have several differently-encoded cards, each with a different level of access authorization. Thus, some cards may access a biographical page without any calendar information, other cards may access the same or different page with access enabled to today's calendar, and still other cards may access the same or different page with access enabled for the card-giver's complete calendar.

The reference to business cards and personal calendars is illustrative only. The invention is more widely applicable. Going back a century, "calling cards" were used by persons whose interests were strictly social, rather than business. The principles of the present invention can similarly be applied. Teenagers can carry small cards that can be exchanged with new acquaintances to grant access to private dossiers of personal information, favorite music, artwork

video clips, etc. The cards can be decorated with art or other indicia that can serve purposes wholly unrelated to the linking data steganographically encoded therein.

Even the "card" paradigm is too restrictive. The same techniques can be applied to any object. A music CD cover can be encoded to point to a promotional site associated with the music artist. A book jacket can link to a similar site. Printed advertising distributed through the US mail (cards, magazines, etc.) can be encoded to point to related web-based promotional sites. (Sponsors of such advertising or other sites can reward visits to their internet site by issuing visitors digital tokens or coupons that can be redeemed for premiums, cash-back, etc., either for any such visit, or only if the visit was effected through the portal of a steganographically-encoded printed medium.)

Many contexts arise in which data to be presented to a consumer is valuable only if timely. The postal service mail is ill-suited for some such information due to the latency between printing a document, and its ultimate delivery to a recipient. The principles of the present invention allow the recipient to take a steganographically-encoded data object (card, etc.) that was printed well before delivery, and use it on receipt to receive up-to-the-minute information. (In this and other embodiments, the steganographically-encoded data can also include data uniquely identifying the recipient/user, so the web site can present data customized to that user.)

The present technology also has application in access control systems. An identification badge (either with photo or graphics, or with text alone) can be encoded with steganographically access control data (e.g., access codes or digital keys) that is recognized by optical-scanner-equipped locks and the like, permitting access by authorized persons to restricted areas or restricted services (e.g., computer privileges). Given the low cost of media and printing (as compared with other access control technologies), the cards can be issued on a daily, weekly, or other frequent interval, and the access control system can be programmed to permit access in response to such cards only for the pre-set limited period. Lost cards soon lose their threat.

Tickets to sporting events, concerts, and other events can be steganographically encoded to permit the bearer to access premium web content available only to those who have purchased tickets (e.g., an on-line text-, audio-, or video-chat session with the featured performer or sports star the day before the event). Alternatively, the encoded data may link to a transactional site. In some such embodiments, the ticket is printed with a nominal show data and seat assignment, but also includes a UID in addition to the encoded address of an associated transactional ticket site. The user then can visit the transactional web site to change seating (or date). On attending the event, the consumer presents the ticket to a steganographic decoder apparatus that discerns the UID and looks up the seat assignment most-recently picked by the consumer. It then prints a chit entitling the consumer to take the seat earlier selected on-line.

The reference to "scanning" of objects naturally brings to mind images of desktop flatbed scanners, or multi-function hydra devices. While such devices can be used—together with convention digital cameras (including video cameras)—the inventors foresee that image input devices will soon be much more commonplace. The provision of digital cameras as built-in components of certain computers (e.g., the Sony Vaio laptops) is just one manifestation of this trend. Another is camera-on-a-chip systems, as typified by U.S. Pat. No. 5,841,126 and detailed in Nixon et al., "256×256 CMOS Active Pixel Sensor Camera-on-a-Chip," IEEE J. Solid-State Circuits, Vol. 31(12), pp. 2046–2051 (1996), and Fossum, "CMOS Image Sensors: Electronic Camera-on-a-Chip," IEEE Transactions of Electron Devices, vol. 44, No. 10, October 1997. Still another is head-mounted cameras (as are presently used in some computer-augmented vision systems). These and other image input devices can all be used in connection with the present invention.

To facilitate embodiments of the present invention, a prior art camera-on-a-chip system can be modified to also include a steganographic watermark detector on the same semiconductor substrate. Such a chip—in addition to providing image output data—can also analyze the image data to discern any steganographically encoded data, and produce corresponding output data. (Again, such analysis desirably includes correction for scale and rotation factors, so precise positioning of the object being "read" is not essential for correct decoding.)

To provide a comprehensive disclosure without unduly lengthening this specification, applicants incorporate by reference the patents, applications, and publications identified above.

APPENDIX B

METHODS AND SYSTEMS EMPLOYING DIGITAL WATERMARKING

Field of the Invention

The present invention relates to applications of digital watermarking in conjunction with audio, video, imagery, and other media content.

Background

Watermarking (or "digital watermarking") is a quickly growing field of endeavor, with several different approaches. The present assignee's work is reflected in U.S. Pat. Nos. 5,841,978, 5,768,426, 5,748,783, 5,748,763, 5,745,604, 5,710,834, 5,636,292, 5,721,788, and laid-open PCT applications WO97/43736 and WO99/10837. Other work is illustrated by U.S. Pat. Nos. 5,734,752, 5,646,997, 5,659,726, 5,664,018, 5,671,277, 5,687,191, 5,687,236, 5,689,587, 5,568,570, 5,572,247, 5,574,962, 5,579,124, 5,581,500, 5,613,004, 5,629,770, 5,461,426, 5,743,631, 5,488,664, 5,530,759, 5,539,735, 4,943,973, 5,337,361, 5,404,160, 5,404,377, 5,315,098, 5,319,735, 5,337,362, 4,972,471, 5,161,210, 5,243,423, 5,091,966, 5,113,437, 4,939,515, 5,374,976, 4,855,827, 4,876,617, 4,939,515, 4,963,998, 4,969,041, and published foreign applications WO 98/02864, EP 822,550, WO 97/39410, WO 96/36163, GB 2,196,167, EP 777,197, EP 736,860, EP 705,025, EP 766, 468, EP 782,322 WO 95/20291, WO 96/26494, WO 96/36935, WO 96/42151, WO 97/22206, WO 97/26733.

Most of the work in watermarking, however, is not in the patent literature but rather in published research. In addition to the patentees of the foregoing patents, some of the other workers in this field (whose watermark-related writings can by found by an author search in the INSPEC database) include I. Pitas, Eckhard Koch, Jian Zhao, Norishige Morimoto, Laurence Boney, Kineo Matsui, A. Z. Tirkel, Fred Mintzer, B. Macq, Ahmed H. Tewfik, Frederic Jordan, Naohisa Komatsu, and Lawrence O'Gorman.

The artisan is assumed to be familiar with the foregoing prior art.

In the present disclosure it should be understood that references to watermarking encompass not only the assign-

ce's watermarking technology, but can likewise be practiced with any other watermarking technology, such as those indicated above.

Watermarking has various uses, but the present specification details several new uses that provide functionality and features not previously available.

Brief Description of the Drawings (omitted from this Appendix)

FIG. **1** is a diagram showing the participants, and channels, involved in the distribution of music.

FIG. **2** shows a conceptual model of how music artists, record labels, and E-Music distributors can all interact with a Media Asset Management System, of which several are detailed in the following specification.

Detailed Description

For expository convenience, much of the following discussion focuses on music, but the same principles and techniques are largely or wholly applicable to other source data, whether non-music audio, video, still imagery, printed materials, etc.

Music Asset Management

Referring to the figures, the music distribution process begins with a creative artist **10**. The artist's music has traditionally been distributed by a record label **12**. (While the following discussion refers to distribution through such a label, it should be understood that such distribution can just as well be effected directed under the artist's control, without a record label intermediary.)

In traditional distribution **14**, the record label produces tangible media, such as records, tapes, videos (eg. music videos), and CDs **16**. These media are physically distributed to end-consumers **18**. Additionally, the label **12** distributes the music media to outlets **20**, such as radio and TV stations, cable and satellite systems, etc., which broadcast (or narrowcast) the artist's work to an audience. Distribution through such media outlets may be monitored by playout tracking services. Playout tracking data, collected by firms including Arbitron, Nielsen, ASCAP, BMI, etc., can be used to compute royalty payments, to verify broadcast (e.g. for advertising), etc.

Increasingly, the distribution of the music to the media outlets is performed electronically. Such distribution first took the form of analog audio over high quality landlines or satellite channels. Digital audio quickly supplanted analog audio in such distribution channels due to higher fidelity.

More recently, distribution of the music from the record labels to the media outlets has occurred over secure links, now including the internet. Such security was first provided simply by scrambling the audio signal or data. More sophisticated "container"-based systems are now coming into vogue, in which the audio is "packaged" (often in encrypted form) with ancillary data.

Electronic distribution of music to the consumer is also gaining popularity, presently in the MP3 format primarily. The music providers may deal directly with the public, but more commonly effect such consumer distribution through a newly emerging tier of digital media outlets, such as internet sites that specialize in music. From such sites, consumers can download digital audio files into personal digital audio players. (The Diamond Rio, and the Audible MobilePlayer devices are some of the first of what will doubtless be a large number of entrants into this personal internet audio appliance market.) Or the downloaded data can be stored by the consumer-recipient onto any other writeable media (e.g. hard disk, CD, DVD, tape, videotape, etc.). Typically a personal computer is used for such downloading, but this intermediary may be dispensed with by coupling next generation of personal audio appliances to an internet-like link.

The data downloaded by the consumer can be stored either in the native digital format, translated into another digital format (which translation may include decryption), converted into analog and recorded in analog form, etc.

Unauthorized copying or use of the music can occur anywhere in the foregoing channels. However, one of the greatest risks occurs once the music has been delivered to the consumer (whether by tangible media, by traditional broadcast media outlets, by emerging digital distribution, or otherwise).

The general idea of embedding auxiliary data into music (i.e. watermarking) has been widely proposed, but so far has been of limited applicability.

For example, GoodNoise is planning to embed a digital signature—termed a multimedia identifier, or MMI—in its MP3 music. MMI will register the song and its author with a licensing number. In addition to providing information about the songwriter and distributor, this digital encoding may also include lyrics, liner notes, and other information. But all of the proposed uses serve only to convey information from the distributor to the consumer; use for "tracking" is actively disclaimed. (Wired News, "GoodNoise Tags MP3 Files," Feb. 3, 1999.)

The Genuine Music Coalition—a partnership of various companies in the music distribution business—likewise has announced plans to employ watermarking of MP3 music. The watermarking technology, to be provided by Liquid Audio, will convey data specifying the artist or producer contact, copyright data, and a number to track ownership. The Coalition hopes that the provision of this embedded information will help thwart piracy. Industry observers believe Liquid Audio will next introduce playback technology only plays audio in which its watermark is detected. (Wired News, "Liquefying MP3," Jan. 23, 1999.)

A similar initiative has been announced by the Recording Industry Association of America (RIAA). Termed the Secure Digital Music Initiative (SDMI), the program seeks to define a voluntary specification that will assure proper compensation to those who produce and distribute music. One element of the system will likely be a watermarking component. (Dow Jones Newswire, "Spurred By Maverick Technology, Music Industry Eyes Web," Dec. 31, 1998.)

Yet another initiative has been announced by Solana and ASCAP. Other companies promoting watermarking for music include Aris Technology, MCY.com, and AudioSoft.

The watermark payload can represent various types of data. An exemplary payload includes data relating to the artist, distribution entity, title, and copyright date/proprietor. Additionally, the payload can include a digital object identifier—an ISBN-like number issued by a central organization (e.g. a rights management organization) to uniquely identify the work.

Such payload data can be encoded literally (e.g. the title by a series of ASCII characters, etc.). In other embodiments, codes or abbreviations can be employed—with each code having a known meaning. In still other embodiments, the data can be meaningless by itself, but may serve as a key (e.g., a Unique Identifier, or UID) into a remote data database or repository. An example of such a remote data repository is a web site at a Master Global Address (MGA) associated with content, as detailed below.

An exemplary data payload may, for example, have the following format:

A	B	C	D	E	F	G	H	I		

Where A is a six-byte (8-bits to a byte) ASCII string serving as a digital object identifier (which may serve as a link to a Master Global Address through a default name server, as discussed below), B is a two-byte ASCII field serving as a key into an "artist" field of the remote database, C is a three-byte ASCII field serving as a key into a "title" field of the remote database; D is a 14-bit field serving as a key into a "label" field of the remote database, E is an 8-bit integer representing the work's year of first publication (with 0 representing the year 2000); F is a 10-bit field serving as a key into a "price" field of the remote database, G is a two-byte usage control string (detailed below), H is a streaming data channel, and I is a string of bits serving as a cyclic redundancy checksum for the foregoing. (More sophisticated error correcting checksums can, of course, be employed.) This payload format totals 136 bits, exclusive of the CRC coding and the streaming data channel.

This payload is encoded repeatedly, or redundantly through the music, so that the full payload can be decoded from partial excerpts of the music.

The encoding is also desirably perceptually adaptive, so that higher energy encoding is employed where the listener is less likely to perceive the additional "noise" introduced by the encoding, and vice versa. Various techniques for perceptually adaptive encoding are known. For example, some tie the amplitude of the encoded signal to the instantaneous amplitude of the music. Others exploit psychoacoustic "masking" of one signal by a spectrally-or temporally-adjoining signal of higher energy. Still other approaches fill gaps in the music's spectrum with watermark energy. These and other techniques are detailed in the patents incorporated by reference.

In other embodiments, perceptually adaptive encoding is not used. In some such embodiments, no tailoring of the temporal or spectral characteristics of the watermark signal is employed. In others, the watermark signal is spectrally filtered to emphasize low frequency audio components (e.g. less than 500 hz), high frequency audio components (e.g. higher than 2500 hz), or mid-frequency audio components (500–2500 hz).

The streaming data field channel (H) is a medium by which data can be conveyed from a distribution site (or other site) to the end user. Such data may be entirely unrelated to the underlying work. For example, it may serve a utilitarian purpose, such as conveying data to a memory in the consumer device to replace previously-stored data that is out-of-date. It may be a commercial channel on which bandwidth is sold for access to the consumer or the consumer's device. Essentially any purpose can be served by this streaming data field. Unlike most of the other fields, the streaming data field may not endlessly repeat the same data, but can convey data that changes with time.

Desirably, the encoding is performed in a manner permitting recovery of the watermark data even if the audio is corrupted, e.g. by format conversion, re-sampling, tape wow and flutter, compression, coding, or various forms of audio processing (e.g. filtering, pre-emphasis, re-scaling, etc.). One way to provide for such robustness is to encode a signal of known character that can be recognized through all such corruption. By identifying such known signal, the watermark signal can then be decoded. (The known signal can take various forms, e.g. a synchronization signal, a marker signal, calibration signal, a universal code signal as described in applicant's patents, etc.)

In some embodiments, a watermark "dial-tone" signal is provided. This dial-tone signal is a low amplitude, relatively wideband, repetitive signal that commonly conveys only limited information (e.g. a single bit of information). Its presence in an audio signal can serve as a "do not record," or similar instruction signal. Alternatively, or in addition, the dial-tone signal can serve as an aid in "locking" to a plural-bit digital watermark signal that is also encoded in the audio. For example, the cyclical repetition of the signal can serve to identify the start of the plural-bit digital watermark signal. Or the spectrum or repetition rate of the signal can identify any temporal corruption of the audio. An exemplary such signal is detailed as a "simple universal code" in U.S. Pat. No. 5,636,292.

A track of music can be pre-authorized for specified types of use. For example, the usage control string of the watermark payload may include a six-bit field detailing the classes of devices for which the audio is authorized. Each bit would correspond to a different class of device. Class 1 devices may be personal playback devices with only analog-audio output. Class 2 devices may be personal entertainment devices capable of outputting music in digital (e.g. MP3, redbook, *. WAV) format, as well as analog audio. Class 3 devices may be personal computer systems (i.e. with essentially unlimited ability for processing and outputting digital audio). Etc., etc. A device to which such MP3 audio is provided would check the usage control string data to determine whether it is authorized to utilize the audio. A personal playback device with analog-only output, for example, would examine the first bit of the usage control string. If it was "1," the device would be authorized to use (i.e. playback) the MP3 data; if it was a "0," the device would refuse to play the music.

In addition to pre-authorization for certain classes of devices, the usage control string can also include bits indicating the number of permitted playbacks. This data can be encoded in bits seven through nine, representing eight possibilities:

0—no playback permitted
1—single playback permitted
2—two playbacks permitted
3—three playbacks permitted
4—four playbacks permitted
5—five playbacks permitted
6—10 playbacks permitted
7—unlimited playbacks permitted
8—refer to associated data (within the watermark, or stored at a remote site) which specifies number of permitted playbacks.

The playback device may include a non-volatile store in which the number of permitted playbacks is stored for each track of music. The device would decrement this number at the beginning of each playback.

The usage control string can also include a two-bit field (bits ten and eleven) indicating recording permissions. A value of 0 means that data corresponding to the MP3 audio (regardless of digital format) should never be made available to another digital device. A value of 1 means that the data corresponding to the MP3 data may be made available once to another digital device. A value of 2 means that the data may be made available an unlimited number of times to other digital devices. (Value 3 is reserved.)

Another data field that can be included in an audio watermark is a rating that indicates age-appropriateness.

Music with violence or sexual themes might be given a rating akin to the MPAA "PG-13" or "R" rating. Audio appliances may be programmed to recognize the rating of incoming music, and to interrupt playback if the rating exceeds a certain threshold setting. Various known techniques can be employed to assure that such settings cannot readily be changed, e.g., by juvenile listeners.

Another data field that can be included in an audio watermark is a date field. This field can indicate either the date the music was watermarked, or a date in the future on which certain rights associated with the music should change. Some consumers, for example may not wish to purchase perpetual playback rights to certain musical selections. The right to play a selection for 6 months may suffice for many consumers, especially if the price is discounted in view of the limited term. Such an arrangement would not be wholly disadvantageous to music distributors, since some consumers may end up purchasing music twice if their initial assessment of a musical selection's appeal was too short-sighted. (Naturally, the playback equipment would require a source of real-time clock data against which the date field in the watermark can be checked to ensure that the playback rights have not yet expired.)

Another of the data fields that can be included in an audio watermark specifies technical playback parameters. For example, the parameter can cause the playback appliance to apply a spectral equalization that favors bass frequencies, or treble frequencies, or mid-range frequencies, etc. Other pre-configured equalization arrangements can similarly be invoked responsive to watermark data. Likewise, the parameter can invoke special-effects provided by the playback appliance, e.g., echo effects, reverb, etc. (Again, such parameters are usually represented in an abbreviated, coded form, and are interpreted in accordance with instructions stored in a memory (either in the playback appliance, or linked thereto).

The same data fields and principles can be applied to non-audio content. In video, for example, watermarked data can adaptively control the display monitor or playback parameters (e.g., color space) to enhance the viewing experience.

Music Asset Management/Commerce

The majority of domestic music piracy is not organized. Rather, it is a crime of opportunity and convenience. If the crime were made more difficult, the alternative of obtaining a copy through legitimate channels would be less onerous. Similarly, if the procedure for obtaining a copy through legitimate channels were simplified, the incentive for piracy would be reduced. Watermarking facilitates both—making the crime more difficult, and making legitimate music acquisition easier.

Consider, for example, the pricing of music in conventional record stores. A CD (compact disk) may cost $15, but its sale may be driven by just one or two popular songs on the disk. To obtain these songs, the consumers must purchase the entire disk, with perhaps a dozen songs of no particular interest. This, in essence, is a tying arrangement that benefits the record labels while prejudicing the consumers. Given these circumstances, and a ready opportunity to make copies, it is not surprising that customers sometimes make illicit copies.

One classic technique of avoiding purchase of a complete collection of music, when only one or two songs is desired, is to record the music off the radio. While of dubious legality, this technique was popular in the era of combined cassette/radio players. However, the desired music was sometimes difficult to encounter in a radio broadcast, and the quality was less than superb.

The combined cassette/radio player has now evolved into a general purpose computer with wide-ranging functionality, and other sophisticated devices. Music can be acquired off the web, and can be recorded in various forms (e.g. in a personal MP3 player, stored on a hard disk, stored on a writeable CD-ROM, played back and recorded on analog cassette, etc., etc.). The quality can be quite high, and the erratic broadcast time problems of radio broadcasts have been overcome by the web's on-demand delivery mechanisms. (Moreover, the music can be downloaded in faster-than-realtime, a further benefit over recording-off-the-air techniques.)

One hybrid between the new and old is a novel radio (e.g., for use in a car) that has a "capture" button on the front panel (or other form of user interface, e.g., a Capture icon on a GUI). If a user hears a song they want to record and keep, they press the Capture button while the song is playing. In response, the radio device decodes a watermark embedded in the music, and thereby knows the identity of the music. The radio then makes a wireless transmission identifying the user and the desired song. A local repeater network picks up the wireless signal and relays it (e.g. by wireless rebroadcast, by modem, or other communication medium) to a music clearinghouse. The clearinghouse charges the user a nominal fee (e.g. via a pre-arranged credit card), and queues the music for download to a predetermined location associated with the user.

In one embodiment, the predetermined location is the user's own computer. If a "live" IP address is known for the user's computer, the music can be transferred immediately. If the user's computer is only occasionally connected to the internet, the music can be stored at a web site (e.g. protected with a user-set password), and can be downloaded to the user's computer whenever it is convenient.

In other embodiments, the predetermined location is a personal music library maintained by the user. The library can take the form, e.g., of a hard-disk or semiconductor memory array in which the user customarily stores music. This storage device is adapted to provide music data to one or more playback units employed by the user (e.g. a personal MP3 player, a home stereo system, a car stereo system, etc.). In most installations, the library is physically located at the user's residence, but could be remotely sited, e.g. consolidated with the music libraries of many other users at a central location.

The personal music library can have its own internet connection. Or it can be equipped with wireless capabilities, permitting it to receive digital music from wireless broadcasts (e.g. from the clearinghouse). In either case, the library can provide music to the user's playback devices by short-range wireless broadcast.

By such arrangement, a user can conveniently compile an archive of favorite music—even while away from home.

Many variants of the foregoing are of course possible. The radio can be a portable unit (e.g. a boombox, a Walkman radio, etc.), rather than an automotive unit. The UI feature employed by the user to initiate capture a musical selection need not be a button (physical or on-screen). For example, in some embodiments it can be a voice-recognition system that responds to spoken commands, such as "capture" or "record." Or it can be a form of gesture interface.

Instead of decoding the watermark only in response to the user's "capture" command, the radio can decode watermarks from all received programs, and keep the most recent in a small FIFO memory. By such arrangement, the user need not issue the capture instruction while the song is playing, but can do so even after the song is finished.

In some embodiments, data corresponding to the watermark can be made available to the user in various forms. For example, it can be presented to the user on an LCD screen, identifying the artist and song currently playing. If a corresponding UI button is activated, the device can so-identify the last several selections. Moreover, the data need not be presented to the user in displayed form; it can be annunciated by known computer-speech technologies instead.

In embodiments in which the watermark does not convey ASCII text data, but instead conveys UIDs, or coded abbreviations, the device must generally interpret this data before presenting it to the user. In an illustrative embodiment, the device is a pocket-sized FM radio and is equipped with a 1 megabyte semiconductor non-volative RAM memory. The memory includes a data structure that serves as a look-up table, matching code numbers to artist names and song titles. When the user queries the device to learn the identity of a song, the memory is indexed in accordance with one or more fields from the decoded watermark, and the resulting textual data from the memory (e.g. song title and artist) is annunciated or displayed to the user.

In most applications, such memory will require frequent updating. The RF receiver provides a ready mechanism for providing such updated data. In one embodiment, the radio "awakens" briefly at otherwise idle moments and tunes to a predetermined frequency at which updated data for the memory is broadcast, either in a baseband broadcast channel, or in an ancillary (e.g. SCA) channel.

In variants of the foregoing, internet delivery of updated memory data can be substituted for wireless delivery. For example, the artist/song title memory in the personal player can be updated by placing the player in a "nest" every evening. The nest (which may be integrated with a battery charger for the appliance) can have an internet connection, and can exchange data with the personal device by infrared, inductive, or other proximity-coupling technologies, or through metal contacts. Each evening, the nest can receive an updated collection of artists/song titles, and can re-write the memory in the personal device accordingly. By such arrangement, the watermark data can always be properly interpreted for presentation to the user.

The "Capture" concepts noted above can be extended to other functions as well. One is akin to forwarding of email. If a consumer hears a song that another friend would enjoy, the listener can send a copy of the song to the friend. This instruction can be issued by pressing a "Send" button, or by invoking a similar function on a graphical (or voice- or gesture-responsive) user interface. In response, the appliance so-instructed can query the person as to the recipient. The person can designate the desired recipient(s) by typing in a name, or a portion thereof sufficient to uniquely identify the recipient. Or more typically, the person can speak the recipient's name. As is conventional with hands-free vehicle cell phones, a voice recognition unit can listen to the spoken instructions and identify the desired recipient. An "address book"-like feature has the requisite information for the recipient (e.g., the web site, IP address, or other data identifying the location to which music for that recipient should stored or queued, the format in which the music should be delivered, etc.) stored therein. In response to such command, the appliance dispatches instructions to the clearinghouse, including an authorization to debit the sender's credit card for the music charge. Again, the clearinghouse attends to delivery of the music in a desired manner to the specified recipient.

Still further, a listener may query the appliance (by voice, GUI or physical button, textual, gesture, or other input) to identify CDs on which the then-playing selection is recorded. Or the listener may query the appliance for the then-playing artist's concert schedule. Again, the appliance can contact a remote database, relay the query, and forward data from the watermark payload identifying the artist and/or song title to which the query relates. The database locates the requested data, and relays same back to the appliance for presentation (via a display, by machine speech, or other output) to the user. If desired, the user can continue the dialog with a further instruction, e.g., to buy one of the CDs on which the then-playing song is included. Again, this instruction may be entered by voice, GUI, etc., and dispatched from the applicance to the clearinghouse, which can then complete the transaction in accordance with pre-stored information (e.g. credit card account number, mailing address, etc.). A confirming message is relayed to the appliance for presentation to the user.

While the foregoing transactions require a link to a remote site or database, other watermark-based consumer services can be provided without such a link. For example, a user can query the appliance as to the artist or song-title of the selection currently playing. The appliance can consult the embedded watermark data (and optionally consult a memory to determine the textual names associated with coded watermark data), and provide the requested information to the user (e.g., by a display, annunciation, or other output).

The foregoing concepts (e.g. Capture, Send, etc.) can also be employed in connection with internet- rather than radio-delivery of music. (The following discussion is illustrated with reference to the "Capture" function, but it will be recognized that the other earlier-discussed features can be similarly implemented.)

There are many commercial web sites that sell audio (in CD form or otherwise), and offer limited free music downloads, (or music clips) as an enticement to lure consumers. But there are also a great number of music web sites that have no commercial pretense. They are hosted by music lovers strictly for the enjoyment of other music lovers. When music is downloaded from such a web site, the end-user's computer can analyze the digital data to decode watermark data therefrom. Again, the user can be provided with a "Capture" button that initiates a commercial transaction, by which a complete copy of the then-downloaded audio is sent to a prearranged storage location, and the user's credit card is debited accordingly. This transaction can occur independently of the site from which the music is downloaded (e.g. through the clearinghouse referenced above).

While the "Capture" button can be presented on the web-site, this would generally not be in keeping with the non-commercial nature of such web sites. Instead, in an exemplary embodiment, the Capture feature is a software program resident at the user's computer. When this software program is invoked by the user, a socket channel is instantiated between the user's computer and the clearinghouse over the then-existing internet connection. The decoded watermark data and user ID is transmitted to the clearinghouse over this channel, without interrupting the user's other activity (e.g. downloading music from the non-commercial web site). In response, the clearinghouse transmits the music to the prearranged location and attends to billing.

In some embodiments, a watermark detector is included as part of the operating system, and constantly monitors all TCP/IP, or other internet, data received by the user's computer, for the presence of watermarks. In such case, when the Capture feature is invoked, the program examines a memory location in which the operating system stores the most-recently received watermark data. In another

embodiment, the computer does not monitor all internet traffic for embedded watermark data, but includes an API that can be called by the Capture program to decode a watermark from the data then being received. The API returns the decoded watermark data to the Capture program, which relays same to the clearinghouse, as above. In still another embodiment, the watermark decoder forms part of the Capture program, which both decodes the watermark and relays it to the clearinghouse when the Capture program is invoked by the user.

There are various techniques by which the Capture program can be selectively invoked. One is by a keyboard macro (e.g. by a combination of keyboard keys). Another is by a program icon that is always presented on the screen, and can be double-clicked to activate. (Again, confirmation processes may be called for, depending on the likelihood of inadvertent invocation.) Many other techniques are likewise possible.

In the just-contemplated scenario, the Capture operation is invoked while the user is downloading music from a non-commercial web site. This seems somewhat redundant, since the downloading—itself—is transferring music to the user's computer. However, the Capture operation provides added value.

In the case of streaming audio, the audio is not typically stored in a location in which it can be re-used by the consumer. It can be listened-to as delivered, but is then gone. Capturing the audio provides the user a copy that can be played repeatedly.

In the case of downloaded music files, the music may have been encoded to prevent its recordal on other devices. Thus, while the user may download the music onto a desktop computer, copy-prevention mechanisms may prevent use of that file anywhere else, e.g. on a portable music appliance. Again, Capturing the audio provides the user a copy that can be transferred to another device. (The music file provided by the clearinghouse can have copy-prevention limits of its own—e.g., the file can be copied, but only once, or the file can be copied only onto devices owned by the user.)

(Confirmation of device ownership can be implemented in various ways. One is to identify to the clearinghouse all music devices owned by a user at the time the user registers with the clearinghouse (supplemented as necessary by later equipment acquisitions). Device IDs associated with a user can be stored in a database at the clearinghouse, and these can be encoded into the downloaded music as permitted devices to which the file can be copied, or on which it can be played.)

The commerce opportunity presented by non-commercial music web-sites is but one enabled by digital watermarks. There are many others.

To take one example, consider the media by which music and artists are presently promoted. In addition to radio airtime, these include music videos (a la MTV), fan magazines, web advertisements, graphical icons (e.g. the Grateful Dead dancing bears), posters, live events, movies, etc. Watermarked data can be used in all such media as a link in a commercial transaction.

A poster, for example, typically includes a photo of the artist, and may comprise cover-art from a CD. The photo/art can be digitally watermarked with various types of data, e.g., the artist's identify, the record label that distributes the artist's work, the music project being particularly promoted by the poster (e.g. a CD, or a concert tour), a fan web-site related to the artist, a web-site hosted by the record label for selling audio in CD or electronic form, a web-site from which free music by the artist can be downloaded, data identifying the poster itself, etc.

A user, equipped with a portable appliance that merges the functions of palmtop computer and digital camera, can snap an image of the poster. The processor can decode the watermarked data, and initiate any of various links based on the decoded data.

In an exemplary embodiment, after snapping the picture, the user invokes a software program on the device that exposes the various links gleaned from the snapped image data. Such a program can, for example, present the option of linking to the artist's fan web site, or downloading free streaming audio or music clips, or ordering the promoted CD, or requesting the above-noted clearinghouse to download a personal copy of selected song(s) by the artist to the user's personal music library, etc. (The device is presumed to have a wireless internet link. In devices not having this capability, the requested actions can be queued and automatically executed when a link to the internet is available.)

Still more complex transactions can be realized with the use of a remote database indexed by digital watermark fields decoded from the poster. For example, the poster may promote a concert tour. Fields of the digital watermark may identify the artist (by a code or full text), and a web site or IP address. The user appliance establishes a link to the specified site, and provides the artist identifier. In response, the site downloads the tour schedule for that artist, for display on the device. Additionally, the downloaded/displayed information can include a telephone number that can be used to order tickets or, more directly, can indicate the class of seats still available at each (or a selected) venue, and solicit a ticket order from the user over the device. The user can supply requested information (e.g. mailing address and charge card number) over the return channel link (wireless or wired, as the case may be), and the ticket(s) will be dispatched to the user. In the case of a wireless link all of this can occur while the user is standing in front of the movie poster.

Similar systems can be implemented based on watermark data encoded in any other promotional media. Consider music videos. Using known TV/computer appliances, watermark data added to such videos can readily be decoded, and used to establish links to audio download, CD-sales, fan club, concert ticket outlet web sites, etc., as above.

Even live events offer such watermark-based opportunities. The analog audio fed to public address or concert speakers can be watermarked (typically before amplification) to encode plural-bit digital data therein. A next generation personal music appliance (e.g. one with a wireless interface to the internet) can include analog record capability (e.g. a built-in microphone, analog-to-digital converter, MP3 encoder, coupled to the unit's semiconductor memory). A user who attends a live event may record an excerpt of the music. The watermark can then be decoded, and the extracted data used to access the links and commerce opportunities reviewed above.

Cinema movies offer both audio and visual opportunities for watermark-based commerce opportunities. Either medium can be encoded to convey information of the types reviewed above. A personal appliance with image- or audio-capture capabilities can capture an excerpt of the audio or imagery, decode the watermark data therefrom, and perform any of the linking, etc., functions reviewed above.

The consumer-interest watermarks reviewed above are only exemplary. Many others will be recognized as useful. For example, promotional clips presented before a feature film presentation can include watermark data that point (either by a literally encoded web address link, or by an ID code that indexes a literal link in a remote link database) to

reviewer critiques of the previewed movies. Watermark data in a featured film presentation can lead to web sites with information about the movie stars, the director, the producer, and can list other movies by each of these persons. Other watermark-conveyed web links can present opportunities to buy the movie on videotape, to purchase the movie soundtrack, to buy movie-related toys and games, etc.

More on Device Control

Much of the foregoing has focused on watermark encoding to provide enhanced customer experiences or opportunities. Naturally, watermarks data can alternatively, or additionally, serve the interests of the media owner.

To illustrate, consider watermarked music. The media owner would be best served if the watermark serves dual purposes: permissive and restrictive. Permissively, music appliances can be designed to play (or record) only music that includes an embedded watermark signaling that such activity is authorized. By this arrangement, if music is obtained from an unauthorized source and does not include the necessary watermark, the appliance will recognize that it does not have permission to use the music, so will refuse requests to play (or record).

As noted, music appliances can respond restrictively to the embedded watermark data to set limits on use of the music. Fields in the watermark can specify any or all of (or others in addition to) (a) the types of devices on which the music can be played (b) the types of devices on which the music can be recorded; (c) the number of times the music can be played; (d) the number of times the music can be recorded, etc.

The device restrictions (a) and (b) can be of various types. In some embodiments, the restrictions can identify particular units (e.g. by serial number, registered owner, etc.) that are authorized to play/record the encoded music. Or the restrictions can identify particular classes of units (e.g., battery-powered portable players with music memories of less than 50 megabytes, disk-based dedicated music appliances, general purpose personal computers, etc.). Or the restrictions can identify particular performance quality criteria (e.g., two channel, 16-bit audio at 44.1 KHz sample rate, or lower quality).

The use restrictions (c) and (d) can likewise be of various types. Examples include "do not copy," "copy once only," "unrestricted copying permitted," "play once," "play N times" (where N is a parameter specified elsewhere in the watermarked data, or by reference to a database indexed by a watermark data field), "unrestricted playing permitted," etc.

It is straight forward to design a music appliance to respond to usage limits of zero (e.g. "do not copy") and infinity (e.g. "unrestricted copying permitted," and "unrestricted playing permitted"). The device simply examines one or more bits in the watermark data, and permits (or refuses) an operation based on the value thereof.

Implementation of the other usage-control restrictions can proceed in various ways. Generally speaking, the stored music can be altered to give effect to the usage-control restrictions. For example, if the music is "record-once," then at the time of recording, the appliance can alter the music in a fashion indicating that it now has "do not record" status. This alteration can be done, e.g., by changing the watermark data embedded in the stored music (or adding watermark data), by changing other data stored in association with the music, etc. If the original signal is stored (as opposed, e.g., to a streaming signal, such as an internet or wireless transmssion), it too should be so-altered.

Likewise with playback limitations. The number of playbacks remaining can, e.g., be encoded in an updated watermark in the music, be tracked in a separate counter, etc.

More particularly considering the "copy once" usage restriction, an illustrative embodiment provides two distinct watermark payload bits: a "copy once" bit and a "copy never" bit. When originally distributed (whether by internet, wireless, or otherwise), the "copy once" bit is set, and the "copy never" bit is un-set.

When music encoded in this fashion is provided to a compliant recording device, the device is authorized to make one copy. (A compliant device is one that recognizes encoded watermark data, and behaves as dictated by the watermark.) When this privilege is exercised, the recording device must alter the data to ensure that no further copying is possible. In the illustrated embodiment, this alteration is effected by the recording device adding a second watermark to both the music, with the "copy never" bit asserted. The second watermark must generally be encoded in an "orthogonal" domain, so that it will be detectable notwithstanding the continued presence of the original watermark. Compliant equipment must then check for both watermarks, and refuse to copy if either is found to have the "copy never" bit asserted.

One advantage to this arrangement is that if the watermark signal has undergone some form of corruption (e.g. scaling or resampling), the first watermark may have been weakened. In contrast, the second watermark will be native to the corrupted signal, and thus be more easily detected. (The corruption may also contribute to the orthogonality of one watermark relative to the other, since the two watermarks may not have precisely the same time base or other foundation.)

An alternative approach is not to encode the "copy never" bit in the original music, but leave this bit (in whatever manifestation) blank (i.e. neither "1" nor "0"). In transform-based watermark techniques, this can mean leaving transform coefficient(s) corresponding to the "copy never" bit un-changed. If the watermarking is effected in the temporal sample domain (or spatial domain, for image data), this can mean leaving certain samples pixels) unmodified. The recording device can then alter the transform coefficients and/or samples as necessary to assert the previously-unencoded "copy never" bit when the permitted recording is made.

In such a system, compliant recording devices check for the "copy never" bit in the sole watermark, and refuse to make a copy if it is asserted (ignoring the value of any "copy once" bit).

A third approach to "copy once" is to set both the "copy once" and "copy never" bits, but set the former bit very weakly (e.g. using lower gain and/or high frequency DCT coefficients that do not survive certain processing). The frail "copy once" bit is designed not to survive common corruptions, e.g., resampling scaling, digital to analog conversion, etc. To further assure that the "copy once" bit is lost, the recording device can deliberately add a weak noise signal that masks this bit (e.g. by adding a noise signal in the frequency band whose DCT coefficient conveys the "copy once" bit). In contrast, the "never copy" bit is unchanged and reliably detectable.

In such a system, compliant devices check for the "copy once" bit in the sole watermark, and refuse to make a copy if it is not detected as set.

These three examples are but illustrations of many possible techniques for changing the rights associated with a work. Many other techniques are known. See, e.g., the proposals for watermark-based copy control systems for digital video at the Copy Protection Technical Working Group, http://www.dvcc.com/dhsg/, from which certain of

the foregoing examples are drawn. See also Bloom et al, "Copy Protection for DVD Video," IEEE Proceedings, Special Issue on Identification and Protection of Multimedia Information, June, 1999.

Scaleability

One feature that is desirable in many detector embodiments is scaleability. This refers to the ability of a detector to scale its computational demands to match the computational resources available to it. If a detector is running on a high performance Pentium III workstation, it should be "doing more" than if the same detector is running on a slow microcontroller. One way scalability can be achieved is by processing more or less chunks of input data (e.g. temporal excerpts of music, or blocks/macroblocks of pixels in a frame of video data) to decode watermarks. For example, an input audio stream might be broken into chunks of one second each. A fast processor may complete decoding of each chunk in less than a second, permitting it successively to process each chunk in the data stream. In contrast, a slow processor may require two and a half seconds to decode the watermark from a chunk. While it is processing a first chunk, the second and third pass by un-decoded. The processor next grabs and processes the fourth chunk, permitting the fifth and sixth to pass by un-encoded.

The detector running on the fast processor is clearly more difficult to "fool," and yields a decoded watermark of higher confidence. But both systems decode the watermark, and both operate in "real time."

The skipping of input data in the temporal (e.g. music or video) or spatial (e.g. image or video) domain is but one example of how scaleability can be achieved. Many other approaches are known to those skilled in the art. Some of these alternatives rely on spending more or less time in the data analysis phases of watermark decoding, such as cross-correlation operations.

Reference has been made to watermarked UIDs as referring to a database from which larger data strings (e.g. web addresses, musician names, etc.) can be retrieved. In some embodiments, the data record referenced by a UID can, in turn, point to several other database records. By such arrangements, it is often possible to reduce the payload of the watermark, since a single UID reference can lead to several different data records.

Production Tools

In the prior art, the watermark embedded in a source material is typically consistent and static through a work—unchanging from beginning to end. But as will be recognized from the foregoing, there are many applications that are better served by changing the watermark data dynamically during the course of the work. According to another aspect of the invention, a production tool is provided that facilitates the selection and embedding of dynamically-changing watermark data. One such embodiment is a software program having a user interface that graphically displays the different watermark fields that are being embedded in a work, and presents a library of data (textually or by icons) that can be inserted into each field, and/or permits the user to type in data to be encoded. Another control on the UI controls the advance and rewind of the media, permitting the user to determine the location at which different watermark data begins and ends. Graphical paradigms known from video- and audio-editing tools can be used to indicate the starting and ending frames/samples for each different watermark payload.

Such a tool can be of the standalone variety, or can be integrated into the desktop audio- and video- production and editing tools offered by vendors such as Avid, Adobe, Jaleo, Pinnacle Systems, SoundForge, Sonic Foundry, Xing Technology, Prosoniq, and Sonic Desktop Software.

Payment-Based Systems

Another aspect of the present invention is the use of anonymous payment tokens that can be used to obtain content on the web. In one embodiment, a token comprises a 128-bit pseudo-random number, to which additional bits identifying an issuing bank (or other issuing institution) are appended. (The additional bits can be the IP address of a web server of the bank, a routing number identifying the bank for electronic wire transfers, or other identifier.) The 128-bit numbers are randomly generated by the bank—commonly as needed—and each represents a fixed increment of money, e.g. ten cents.

A consumer wishing to have a store of currency for such commerce pays the bank, e.g., $10 in exchange for 100 tokens. These tokens are transferred electronically to disk or other storage in the consumer's computer in response, e.g., to a credit card authorization, or may be provided by diskette or other storage medium over the counter at a bank branch (in which case the consumer thereafter copies the numbers into storage of his or her computer). (Outlets other than banks can of course be employed for distributing such numbers, much in the manner that convenience and many grocery stores commonly issue money orders.)

Imagine that the consumer wishes to view the final quarter of a Trailblazer basketball game that aired on television a week ago. (The consumer may have either missed the game, or may have seen it but wants to see the last quarter again.) The user directs a web browser to a web site maintained for such purpose and performs a search to identify the desired program. (Typically, the web site is maintained by the proprietor that holds the copyright in the material, but this need not be the case. Some material may be available at several web sites, e.g., maintained by ABC Sports, the National Basketball Association, and Sports Illustrated.) The search can use any of various known search engines, e.g., Infoseek, Verity, etc., and can permit searching by title terms, keywords, date of airing, copyright owner, etc. By typing in, e.g., the keyword 'Trailblazers' and the date 'Apr. 26, 1999,' the consumer is presented a listing of videos available for download. One, hopefully, is the requested game. With each listing is an indication of an associated nominal charge (e.g. 80 cents).

On clicking on a hypertext link associated with the desired basketball game, the viewer is presented a further screen with one or more options. The first of the listed options is the entire game, with commercials. The charge is the nominal charge presented on the earlier screen (i.e. 80 cents). Other options may include the first, second, third, and fourth quarters of the game individually, each of which—save the last, costs 20 cents. The last may be charged at a premium rate, e.g., 30 cents. Clicking on the desired video option yields a further screen through which payment is effected.

To pay for the requested video, the consumer instructs his or her computer to transfer three of the earlier-purchased tokens over the web to the video provider. Various user interface metaphors can be employed to facilitate this transfer, e.g., permitting the user to type the amount of money to be transferred in a dialog box presented on-screen, or dropping/dragging icons representing tokens from an on-screen "wallet" to an on-screen "ticket booth" (or over an icon or thumbnail representing the desired content), clicking on an "increment" counter displayed adjacent the listing of the content, etc. Once the consumer has authorized a transfer of sufficient tokens, the consumer's computer sends to the

web site (or to such other web address as HTML encoding in the viewed web page may indicate) the tokens. This transmission simply takes the form of the three 128+ bit numbers (the '+' indicating the bank identifier)—in whatever packet or other format may be used by the internet link. Once dispatched in this manner, the tokens are deleted from the user's computer, or simply marked as spent. (Of course, in other embodiments, a record of the expenditure may be stored in the consumer's computer, e.g., with the token contents and a record of the audio or video purchase to which they were applied.)

Since the amount of money is nominal, no encryption is provided in this embodiment, although encryption can naturally be provided in other embodiments (e.g., either in sending the tokens from the user to the web site, or earlier, in sending the tokens to the user). As will be seen, provided that the media provider immediately sends the tokens to the bank in real time, encryption is a nice feature but not mandatory.

On receipt of the token data, the web site immediately routes the token data to the identified bank, together with an identifier of the media provider or account to which the funds represented thereby are to be credited. The bank checks whether the 128-bit numbers have been issued by that bank, and whether they have already been spent. If the numbers are valid, the bank updates its disk-based records to indicate that the three tokens have been spent and that the bank now owes the media supplier 30 cents, which it may either pay immediately (e.g., by crediting to an account identified by the media provider) or as one lump sum at the end of the month. The bank then sends a message to the web site confirming that the tokens were valid and credited to the requested account. (Optionally, a message can be sent to the purchaser of the tokens (if known), reporting that the tokens have been redeemed.)

In response, the web site begins delivery of the requested video to the consumer. In the illustrated embodiment, the video is watermarked prior to delivery, but otherwise sent in unencrypted fashion, typically in streaming format, but optionally in file format. (Encryption can be used in other embodiments.) The watermarking in the illustrated embodiment is accomplished on-the-fly and can include various data, including the date of downloading, the download site, the destination IP address, the identity of the purchaser (if known), etc.

The large size of the video and the small charge assessed therefore provide disincentives for the consumer making illicit copies. (Especially as to archival material whose value decays with time, there is not much after-market demand that could be served by illicit copies, making third party compilation of such material for re-distribution financially unattractive. First run video, and material that keeps a high value over time, would not be as well suited for such distribution, and could better employ technology disclosed elsewhere herein.)

In some embodiments, the integrity of the received video is checked on receipt. This feature is described below in the section entitled Watermark-Based Receipts.

In the illustrative system, nothing in the tokens indicates the identity of the purchaser. The web site knows the IP address of the site to which video was delivered, but need not otherwise know the identity of the purchaser. The bank would probably maintain a record of who purchased the tokens, but need not. In any event, such tokens could thereafter be exchanged among consumers, resulting in anonymity from the bank, if desired.

As described above, the video excerpts from which the consumer can select include commercials. At some sites, video may be provided from which the commercials have been excised, or which is delivered in a manner that skips past the commercials without transmitting same to the consumer. Such video will naturally command a premium price. In some embodiments, the difference in price is electronically credited as compensation to accounts maintained for (or by) the advertisers, whose advertisements are not being viewed by such consumers. (The identification of advertisers to be credited is desirably permanently encoded in the video, either throughout the video (if the video has had the commercials removed therefrom), or by data in the commercials themselves (which commercials are skipped for transmission to the consumer, but can still be decoded at the video head-end. Such encoding can be by in-band watermarking or otherwise.)

While the foregoing discussion particularly considered video as the desired content, the same principles are equally applicable in connection with audio, still imagery, and other content.

The token-based payment method is but one of many that can be employed; the literature relating to on-line payment mechanisms is extensive, and all such systems can generally be here-employed.

Tracking 128-bit tokens can be a logistical problem for the bank. One approach is to have a memory with 10^{128} locations, and at each location store a two-bit value (e.g. 00=never issued; 01=issued but not spent; 10=issued and spent; 11=reserved). More complete data could alternatively be stored, but such a memory would be impractically large.

One alternative approach is to hash each 128-bit number, when issued, to a much smaller key value (e.g. 20 bits). A memory with 10^{20} locations can be indexed by this key. Each such location can include four data: an issued 128-bit token number that hashes to that value, first and second date fields indicating the date/time on which that token was issued and redeemed, respectively, and a link specifying the address of a next memory location. That next memory location (outside of the original 10^{20} locations) can include four more data, this time for a second issued-128-bit token number that hashed to the original key value, two date fields, and again with a link to a subsequent storage location, etc.

When a 128-bit random number is generated, the original memory location indexed by the hash code of that number is checked for an earlier number of the identical value (to avoid issuance of duplicate tokens). Each successive location in the linked chain of memory locations is checked for the same 128-bit number. When the end of the linked chain is reached, the bank knows that the 128-bit random number has not previously been issued, and writes that number in the last-addressed location, together with the date of issuance, and a link to a next storage location.

When a 128-bit token is received, the same linked-list processing occurs to identify a first location, and to thereafter step through each subsequent location until a match is found between the token number and the number stored in one of the linked memory locations. When found, that number is marked as redeemed by writing a redemption date/time in the corresponding field. If the search reaches the end of the linked chain without finding a match between the stored numbers and the token number, the token is treated as invalid (i.e. not issued by that bank).

Other manners of tracking the large number of possible token numbers can of course be used; the foregoing is just exemplary. Or the tokens needn't be tracked at all. Such an arrangement is highly practical if the token has sufficient bits. With the illustrated 128 bits, for example, the chance of two identical tokens being issued is infinitesimally small, so

checking for duplicate issuance can be omitted if desired In such case, the bank can simply maintain an ordered list of the token numbers still outstanding and valid. As new tokens are dispensed, their token numbers are added to the list. As tokens are redeemed, their numbers are deleted from the list. Known list processing techniques can be employed to speed such search, update, and delete actions.

Watermark-Based Receipts

Pay-for-content applications commonly assume that if content is transmitted from a server (or head-end, etc.), it is necessarily received. Sometimes this assumption is wrong. Network outages and interruptions and internet traffic load can diminish (e.g., dropped video frames), or even negate (e.g., failed delivery), expected consumer enjoyment of content. In such cases, the consumer is left to haggle with the content provider in order to obtain an adjustment, or refund, of assessed charges.

Watermarks provide a mechanism for confirming receipt of content. If a watermark is detected continuously during a download or other delivery event, a software program (or hardware device) can issue an electronic receipt attesting that the content was properly delivered. This receipt can be stored, and/or sent to the content distributor to confirm delivery.

In one embodiment, a content receiving device (e.g., computer, television or set-top box, audio appliance, etc.) periodically decodes a watermark from the received content to confirm its continued reception. For example, every five seconds a watermark detector can decode the watermark and make a record of the decoded data (or simply record the fact of continued detection of the same watermark). When a changed watermark is detected (i.e., reception of a different content object begins), the duration of the previously-received content is logged, and a receipt is issued.

In a related embodiment, the last portion (e.g., 5 seconds, frame, etc.) of the content bears a different "end of content" watermark that triggers issuance of a receipt. Such a watermark can indicate the length of the content, to serve as a cross-check against the periodic watermark polling. (E.g., if periodic sampling at 2 second intervals yields 545 samples corresponding to the same content, and if the "end of content" watermark indicates that the content was 1090 seconds long, then receipt of the entire content can be confirmed.)

In another embodiment, the watermark can change during the course of the content by including, e.g., a datum that increments every frame or other increment of time (e.g., frame number, time stamp, etc.). A watermark detector can monitor the continued incrementing of this datum throughout the content to confirm that no part was garbled (which would destroy the watermark) or was otherwise missing. Again, at the end of delivery, the receiving system can issue a confirmation that XXX frames/seconds/etc. of the identified content were received.

One application of such technology is to bill for content based on receipt, rather than transmission. Moreover, billings can be adjusted based on percentage of content-value received. If delivery is interrupted mid-way through (e.g., by the consumer disabling the content-receiving device), the nominal billing for the content can be halved. Some prolonged content, e.g., televised/web-broadcast university classes, cannot be "consumed" in one session, and are thus particularly well suited for such pay-as-you-consume billing.

Another application of such technology is in advertising verification. Presently, ads are tracked by transmission or, less frequently, by detection of an embedded code on receipt (cf., Nielsen Media Research's U.S. Pat. Nos. 5,850,249 and 5,737,025). However, such reception-detectors—once triggered—generally do not further note the length of time that the advertising was received, so the same data is produced regardless of whether only five or fifty seconds of a commercial is presented. Watermark monitoring as contemplated herein allows the duration of the advertising impression to be precisely tracked.

In one application of this technology, recipients of advertising are provided incentives for viewing advertising in its entirely. For example, a content-receiving device can include a watermark detector that issues a receipt for each advertisement that is heard/viewed in its entirety. These receipts can be redeemed, e.g., for content tokens as described elsewhere herein, for monetary value, etc. In some embodiments, receipts are generic and can all be applied to a desired premium, regardless of the advertisements through which they were earned. In other embodiments, the receipts are associated with the particular advertisers (or class of advertisers). Thus, a TV viewer who accumulates 50 receipts from advertising originating from Procter & Gamble may be able to redeem same for a coupon good for $2.50 off any Procter & Gamble product, or receipts from Delta Airlines may be redeemed for Delta frequency flier miles (e.g., at a rate of one mile per minute of advertising). Such incentives are particularly useful in new forms of media that give the consumer enhanced opportunities to fast-forward or otherwise skip advertising.

(Although the foregoing "receipt" concept has been described in conjunction with watermark data (and use of watermark technology is believed to be inherently advantageous in this application), the same principles can likewise be implemented with ancillary data conveyed by other means.)

Master Global Address

As suggested above, it is desirable that each piece of content have a web address (the "Master Global Address" (MGA), or "Master IP Address") associated with it. Such address is typically conveyed with the content, e.g., by an IP address watermarked therein.

Consider a consumer who downloads a streaming video having an English language soundtrack. The viewer may not speak English, or may otherwise prefer to listen to the soundtrack in another language. The user can decode the watermark data embedded in the video and initiate a link to the associated web address. There the user is presented with a list of soundtracks for that content object in other languages. The viewer can click on the desired language and receive same via a second simultaneous transmission (e.g., a second socket channel). The consumer's audio/video appliance can substitute the desired audio track for the default English track.

If the streaming video and the alternative soundtrack are hosted on the same server, synchronization is straightforward. The process governing transmission of the alternative soundtrack identifies the process that is streaming video to the same IP address. Based on SMPTE, or other time frame data, the former process syncs to the latter. (If the two data streams don't originate through the same server, time/frame data can be relayed as necessary to the alternative soundtrack server to effect synchronization.)

Another application of the Master Global Address is to serve as a point to which monitoring stations can report the presence, or passage, of content. Consider, for example, a copyright-aware node through which content signals pass, e.g., a computer node on a network, a satellite transponder, etc. Whenever the node detects passage of a media object

(e.g., by reference to a file extension, such as MP3, JPG, AVI, etc.), it sends a "ping" over the internet to the address encoded in the object, simply reporting passage of the object. Similar monitoring facilities can be provided in end user computers, e.g., reporting FileOpen, FileSave, Printing, or other use of content bearing MGA data.

This system can be expanded to include "ping" and "pong" phases of operation. When a software application (or a user appliance, such as a video or audio playback device) encounters a media object (e.g., at time of file open, at time of playback, etc.), it pings the MGA site to report the encounter. The MGA site "pongs" back, responding with instructions appropriate to the encounter. For example, if the object requires payment of a fee before full functionality or access is to be granted, the MGA site can respond to the application with instructions that the object be used (e.g., played back) only in some crippled state preventing the user's full enjoyment (e.g., impaired resolution, or impaired sound quality, or excerpts only, etc.). The MGA site can also inform the user application of the terms (e.g., payment) by which full functionality can be obtained. The application can graphically or audibly present such information to the user, who can authorize a payment, if desired, so that the content can be enjoyed in a less- (or un-) crippled state. On receipt of the payment authorization, the MGA site can inform the user application that enhanced access/usage rights have been purchased, and that the application may proceed accordingly.

Yet another application of the MGA is to present the user of a content object a menu of options that is customized to that object.

In current graphical operating systems, when a user clicks on an icon (e.g., with the right mouse button), a menu is presented detailing actions that can be undertaken in connection with the icon, or the file represented thereby. Such options are pre-programmed (i.e., static), and are typically determined by the operating system based solely on the file extension.

In accordance with this aspect of the present invention, clicking on an icon representing a media object initiates an internet link to the MGA site associated with the object. The MGA site responds with data that is used to customize the menu of options presented to the user in connection with that particular object.

Consider an icon representing a JPG image file. Right-clicking on the icon may yield a menu that gives the user various options presented by the operating system (e.g., delete, compress, rename), and additional options customized in accordance with data from the object's MGA site. These customized options may include, e.g.,

(a) open in 100×150 pixel format for free;

(b) open in 480×640 pixel format for ten cents;

(c) open in 960×1280 pixel format for twenty cents;

(d) purchase rights to use this image in a newsletter having a circulation of under 1000 for $1.25;

(e) display a complete listing of license options.

Clicking on options (b) or (c) initiates a commerce application through which funds are electronically transferred to the MGA site (by the above-described tokens or otherwise). In response, the MGA site responds (e.g., with TCP/IP or HTML instructions) authorizing an application on the user's computer to open the file in the requested manner. (The default application for JPG applications can then automatically be launched, or the computer may first query the user whether another application should be used instead.)

Clicking on option (d) proceeds as above, and permits full use of the image on the computer. Moreover, the MGA site sends a digital certificate to the user's computer memorializing the usage rights purchased by the consumer.

In this particular arrangement, no access control is placed on the content, e.g., by encryption, secure container technology, or the like. The nominal fees, and the ease of licensing, make it simple for the user to "do the right thing" and avoid copyright liability. In other embodiments, of course, known access control techniques can be used to limit use of the object until the requisite payment has been made.

Naturally, records of all such transactions are also logged at the MGA site.

Clicking on option (e) opens a browser window on the user's computer to a web site that presents a complete listing of license options available for that image. (The address of this web site is included in customization data relayed to the user device from the MGA site, but not explicitly shown to the user on the menu.) Through such web site, the user can select desired rights, effect payment, and receive the necessary authorization for software applications on the user's computer (or other media appliance) to open and/or process the content.

The object on which the user "clicks" needn't be an icon. It can be an image or other graphical representation. (And a "click" isn't necessary; a voice command or other signal may be used to the same effect with an audio clip or selection.)

Consider the popular merchandising of books and CDs over the internet. A JPG or other image file depicting the cover of a book, or the artwork of a CD cover, can be treated as a media object, and can include a watermarked MGA pointer. Right-clicking on such an image of a book cover could, through the MGA site, present to the user a menu of options that includes—in addition to those normally presented in conjunction with a JPG file—the following:

(a) "See the review of this book published in the New York Times on Apr. 19, 1999"

(b) "See the list of reviews of this book at Amazon.com"

(c) "Enter your own review of this book, for posting on Amazon.com"

(d) "See today's sales rank of this book at Amazon.com"

(e) "Purchase this book from Amazon.com for $16.95"

(f) "Purchase this book from Barnesandnoble.com for $19.95 and receive a $5.00 credit towards your next purchase"

(g) "Link to the web site that tells about the release of this title as a motion picture (presently scheduled to open on Oct. 10, 1999)"

(h) "Link to the Yahoo listing of web sites relating to this book"

(i) "Search Lycos for listings relating to this book."

If the user selects one of the purchase options from the menu, a pre-stored e-commerce profile—containing the user name, credit card number, billing address, ship-to address, etc., possibly in the form of an encrypted object—could be sent to the MGA site (or to the bookseller) to effect the purchase, or such selection could initiate display of additional screens or sub-menus through which the user would manually enter or select such information for transmission.

Others of the selections cause a new browser window to open on the user's computer, opening to a URL specified in data relayed from the MGA site but not displayed to the user in the menu. Appropriate HTML instructions can be generated to effect a particular query or other operation at the specified URL.

In some embodiments, the customized menu presents only a single choice in addition to those normally provided by the operating system, e.g., "Link to home." Clicking on this option opens a browser window to a home page at the MGA for that object. On that page, the user is presented with all of the foregoing options, and more (possibly including advertising graphics or multi-media). Such objects can serve as powerful marketing agents. Returning to the example discussed above, a JPG image file of a book cover may have, as its MGA, a web page hosted by a particular bookseller, providing purchase options and other information for that book. Marketing of books (or CDs, or cars, or consumer appliances, or virtually anything else) can be effected by disseminating such vendor-issued JPGs as widely as possible. Some book cover JPGs may be distributed by Amazon.com, others by Barnes&Noble.com, others by Borders.com—each pointing back to a different MGA through which purchase transactions for that book may be performed.

Returning to the MGA-customized menus, these needn't be limited to menus resulting from clicking on an icon or image (or signaling during an audio excerpt). Drop-down menus in application programs can likewise be populated with customized options, in accordance with customization data obtained from the MGA site for the object presently being accessed or used. Most graphical operating systems and application programs have well developed toolsets permitting such menu customization. Again, other data relayed from the MGA site is not shown to the user, but is employed by the computer (e.g., a browser program) to carry out menu options selected by the user.

Again the foregoing techniques are equally applicable for still images, audio, video, and other forms of content, and can readily be adapted for use both with general purpose computers, software applications, and specialized media appliances.

While, for expository convenience, the foregoing discussion contemplated embedding a literal URL address in the object as the MGA, more typically this is not the case. Instead, the MGA more commonly comprises identification data for the object (e.g. a 128-bit random ID), together with the URL for a name server computer that serves many (perhaps millions) of such objects (an example of the latter is the Digimarc MarcCentre server).

To obtain the desired data as detailed above, the user's computer (sometimes termed a client computer) links to the name server computer and provides the ID of the object being processed. The name server computer uses this ID to query a database, and obtains from the database the current IP address to which such queries should be routed. The name server computer can relay the request from the client computer to the correct destination address, or can return the correct destination address to the client computer, which can initiate such a link itself. By such arrangement, the IP address ultimately associated with an object can be easily changed as needed, simply by changing the corresponding record in the name server database, without rendering obsolete legacy objects having out-of-date addresses encoded therein.

In some embodiments, the URL of the name server needn't be included in the watermark In the absence of a specified URL, the client computer may direct such links to a default name server address instead (stored locally or remotely). If that server doesn't recognize the object ID, it can return an error code, or pass the query on to other name servers. Those servers, in turn, can pass the query along to still other name servers if they don't recognize the object ID.

In this fashion, an exponentially-large number of name servers might be quickly polled for information relating to the identified object. Alternatively, rather than encoding the complete IP address of the name server in an object watermark, the first N (e.g., 16) bits of the object ID might be used as a short-hand for one of 65,536 predetermined name server addresses, in accordance with data stored locally (e.g., on RAM or disk in the user's computer) or remotely (e.g., at a default name server IP address).

While the basic concept idea behind embedding MGA data within an object is to point to a repository of data about the object, a pointer the other way may be achieved as well.

As noted, the "ping" application of MGA data permits an MGA site to be informed of sites through which its object passes. More generally, the MGA site can log the originating address of each query it receives. Each such address can be presumed to have (or have had) a copy of the corresponding object. Media owners can thereby track the dissemination of copies of their media objects—at least insofar as use of such objects entails communicating with the associated MGA site.

Such tracking offers a great number of opportunities, some in the area of commerce. The MGA site corresponding to the cover art of a Garth Brooks CD, for example, can provide a listing of IP addresses of persons interested in that CD. Email or promotional data objects (e.g., audio clips) can be sent to that list of addresses when a subsequent Garth Brooks CD is released.

Such tracking also opens up a new dimension of internet searching. Presently, internet search engines use a brute force approach, visiting millions of pages across the web in order to identify, for example, a dozen instances of a given photograph file. MGAs offer a shortcut to such brute force approaches. With the present technology, a search engine can find a single instance of a photograph file and, by detection of the MGA data watermarked therein, link to the corresponding MGA site. From the MGA site, the search engine can obtain a listing (if such queries are authorized) of some or all of the other sites known by the MGA site to have copies of that photograph file. (Providing such data to search engines is a commerce opportunity for such MGA sites, which may permit such access to its listing of sites only in exchange for a fee. Or the MGA site may arrange to collect a tribute payment from the search engine proprietor each time the engine responds to a user query using data collected from the MGA site.)

Many of the addresses logged by the MGA may not be publicly-accessible data stores. The search engine can check each listed address to ensure that the desired object is present and accessible before adding the address to its database.

Covert Tracing

Co-pending application Ser. No. 09/185,380 describes anti-counterfeiting technology that looks for the presence of digital data corresponding to bank note imagery in a computer system, and makes a covert record of any attempt to process such data (e.g., Scan, FileOpen, FileSave, Print, Edit, etc.). Such records are hidden from the user of the system (using, e.g., various data encryption and obscuring techniques), but authorized law enforcement officials are provided tools by which these records can be recovered. The forensic data thereby obtained may prove useful in prosecuting counterfeiters. (Knowledge that a computer may be covertly storing evidence of attempted counterfeiting actions may prove as, or more, valuable in deterring counterfeiting than the covert records themselves.)

The same techniques can be employed to deter unauthorized processing of audio, image, video, or content by media

pirates. In one embodiment, a computer's operating system (including peripheral device drivers) monitors various data within the system (e.g., data sent to writeable storage media, or sent via a serial port or network connection, etc.) for data bearing a do-not-copy watermark The presence of such data being sent, e.g., to a writeable disk or to a remote computer, indicates that the do-not-copy instruction has been circumvented. In such case, the operating system writes one or more covert records memorializing the activity, for possible use in criminal prosecution if the computer is lawfully seized.

The example just-provided is but one of many monitoring and response techniques that may be employed to deter circumvention of copy-protection or other access control systems. Generally speaking, if content data is found where it shouldn't be, or is found used as it shouldn't be used, a corresponding record should be made. (Other intervention actions can be triggered as well; covert tracing is desirably just one of several parallel responses to suspected hacking.)

Meta-Data Accessed Using Watermarks

Meta-data, in formats known as SGML, SGML, and HTML, is widely used to communicate information about digital objects (e.g., author, keywords, price, rights, caption, etc.). More generally, meta-data can be thought of as any data construct which associates the name of a property (e.g., "author), with the value of the property (e.g., "Mark Twain"). Such data commonly appears in a tag format, such as the following:

<META NAME="author" CONTENT="Mark Twain">

Meta-data is commonly exchanged between server and client computers in conjunction with the digital objects to which they relate (e.g., the text of a Mark Twain book).

As detailed herein, an important application of watermarking is likewise to convey information about media—in this case embedded within the media content itself (e.g., providing unique identification, establishing some basic behaviors such as do not copy, and providing links to extended functionality).

For meta-data to be useful, it must be linked to associated content, whether in the context of a browser, application program, operating system, asset management system, search engine, etc. However, as detailed below, the content and the associated meta-tags needn't always be conveyed together.

Consider an application program or other client process that receives a watermarked media object. The watermark includes an MGA for that object (which, as noted above, may not specify an ultimate IP address). Stored at the MGA site is meta-data corresponding to the object. By linking to the MGA site identified by the object's watermark, the client computer can obtain the meta-data corresponding to the object. This data can be stored at the client computer and used just as any other meta-data, e.g., to define the local functions that should be available for use with that object (e.g., buy, search, etc.).

A particular example is an on-line catalog of stock photography. Each photograph is watermarked with MGA data. To identify the photographer, copyright date, price, telephone number, subject, etc., an application program can link to the MGA site for that photograph, and obtain the corresponding meta-data. This data can then be displayed or used as needed. Data objects of disparate formats thus can readily be handled within a single, simple application program, since the program needn't concern itself with the varying formats for the associated meta-data (assuming the name servers provide this data in standardized format). Substantial flexibility in programming and object formatting is thereby achieved.

Returning to the internet search engine example described above, MGAs may become recognized as repositories rich in meta-data for media objects. Specialized search engines may focus their data collection around such sites, and be able to quickly identify the MGA sites corresponding to various boolean combinations of meta-tag parameters.

Asset Management/Containers

Much has been written on the topic of asset rights management. Sample patent documents include U.S. Pat. Nos. 5,892,900, 5,715,403, 5,638,443, 5,634,012, 5,629,980 and laid-open European application EP 862,318. Much of the technical work is memorialized in journal articles, which can be identified by searching for relevant company names and trademarks such as IBM's Cryptolope system, Portland Software's ZipLock system, the Rights Exchange service by Softbank Net Solutions, and the DigiBox system from InterTrust Technologies.

An exemplary asset management system makes content available (e.g. from a web server, or on a new computer's hard disk) in encrypted form. Associated with the encrypted content is data identifying the content (e.g. a preview) and data specifying various rights associated with the content. If a user wants to make fuller use of the content, the user provides a charge authorization (e.g. a credit card) to the distributor, who then provides a decryption key, allowing access to the content. (Such systems are often realized using object-based technology. In such systems, the content is commonly said to be distributed in a "secure container.")

Desirably, the content should be marked personalized/serialized) so that any illicit use of the content (after decryption) can be tracked. This marking can be performed with watermarking, which assures that the mark travels with the content wherever—and in whatever form—it may go. The watermarking can be effected by the distributor—prior to dissemination of the encrypted object—such as by encoding a UID that is associated in a database with that particular container. When access rights are granted to that container, the database record can be updated to reflect the purchaser, the purchase date, the rights granted, etc. An alternative is to include a watermark encoder in the software tool used to access (e.g. decrypt) the content. Such an encoder can embed watermark data in the content as it is released from the secure container, before it is provided to the user. The embedded data can include a UID. This UID can be assigned by the distributor prior to disseminating the container. Alternatively, the UID can be a data string not known or created until access rights have been granted. In addition to the UID, the watermark can include other data not known to the distributor, e.g. information specific to the time(s) and manner(s) of accessing the content.

As noted earlier, access rights systems can be realized with watermarks without containers etc. For example, in a trusting world, copyrighted works can be freely available on the web. If a user wishes to make lawful use of the work, the user can decode its watermark to determine the work's terms and conditions of use. This may entail linking to a web site specified by the embedded watermark (directly, or through an intermediate database), which specifies the desired information. The user can then arrange the necessary payment, and use the item knowing that the necessary rights have been secured.

Remote Reconfiguration of Watermark Detectors

In some cases, it is desirable to reconfigure watermark detectors remotely. Such functionality is desirable, for example, if a watermark system is hacked or otherwise compromised.

In accordance with this aspect of the present invention, some aspect of a watermark detector's operation is changed

in response to a command. The change can take various forms. In watermark systems employing pseudo-random key data (e.g., spread spectrum spreading signals), the pseudo-random signal used for detection can be changed. In systems using DFT processing, the mapping between message bits and DFT coefficients can be changed. In still other systems, the decoding can proceed as before, but the significance of one or more bits can be changed (e.g., bits that were normally interpreted as defining Field A can be interpreted as defining Field B, and vice versa). In yet other systems, the decoding can proceed as before, but the response of a device to a given watermark signal can be changed. In still other systems, a set of software instructions can be re-written or re-ordered to effect a change in detector operation.

The command can be conveyed in various ways. In one embodiment, it can be a trigger bit in the watermark payload. Normally the bit has a value of "0." If the bit has a value of "1," the detector system responds by changing its operation. A trigger pattern can also be established, so that detection of a certain combination of bits in the watermark payload serves to trigger the change. Reserved states of certain data fields are examples of patterns that might be employed.

The command can also be conveyed through another channel different than the watermark channel (e.g., an SCA channel of an FM broadcast, or the sub-titling data channel of video broadcasts, or header data within an MPEG data stream, etc., etc.).

The change can proceed in accordance with a pre-programmed rule (e.g., codes progressing successively through a numerically or algorithmically-determined progression), or the change can proceed in accordance with data specified elsewhere in the payload of the watermark bearing the trigger bit (e.g., instead of being interpreted in normal fashion, the non-trigger bits of the detected watermark can define a new pseudo-random key data. Or the change can proceed in accordance with data conveyed in successively-presented watermark payloads, as might be done in video encoding where each frame of video can convey further watermark information. (This latter arrangement is one offering a high-bandwidth re-programming channel through which, e.g., extensive firmware instructions might be transferred to the detector to replace instructions earlier stored.)

By such arrangements, greatly increased detector versatility and functionality can be achieved.

Conclusion

Many diverse embodiments are reviewed above—each with a unique set of features. (Still others are disclosed in the assignee's patents incorporated by reference.) This specification should be construed as explicitly teaching that features illustrated in one such embodiment can generally be used in other embodiments as well. Thus, for example, a date field was not particularly discussed in connection with payload data for video watermarking. Nor were "play once" watermarks so-considered. The inclusion of a calibration signal with (or as part of) the watermark is shown in embodiments of the issued patents, but is not belabored in the above-described embodiments. Likewise with "simple universal codes." The pre-stored commerce profile described in one of the foregoing embodiments is equally applicable to other embodiments as well. Likewise, the presentation of advertising was discussed in connection with one embodiment but not others, although it, too, is generally applicable. All of these concepts are familiar at Digimarc and are regarded as generally applicable throughout the work expressed in Digimarc's patent disclosures. Practicality prevents an exhaustive recitation of each individual permutation and combination.

Having described and illustrated the principles of our invention with reference to illustrative embodiments, it will be apparent that the detailed arrangements can be modified in arrangement and detail without departing from such principles.

For example, while reference has been made to various uses of wireless, it should be understood that such reference does not just cover FM broadcast, and wireless internet networking and the like, but also includes other wireless mechanisms. Examples include cell phones and direct satellite broadcast.

Likewise, while certain embodiments were illustrated with a watermark payload of 100+ bits, in other systems much smaller (or sometimes larger) payloads are desirable—sometimes as small as 1–8 bits.

While the foregoing examples have each been illustrated with reference to a particular media type (e.g., video, audio, etc.), it will be recognized that the principles of each embodiment find application with the other media types as well.

Certain of the appliances contemplated above require user interfaces more sophisticated than are presently typical on such devices. The simplicity of the underlying audio appliance can be preserved, in many instances, by using a palmtop computer—coupled by infrared or otherwise—as a temporary user interface to the appliance. Some of the processing capability can likewise be off-loaded to an ancillary palmtop. (Palmtop is here meant to refer generally to any pocket-size programmable computing device.) Unless otherwise stated, it should be understood that the digital music, video, and imagery contemplated herein is not of any particular form or format. Audio, for example, can be of various forms, both streaming and non-streaming, and of various formats (e.g. **MP3**, **MP4**, MS Audio, Windows Media Technologies, RealAudio, *.WAV, MIDI, Csound, Dolby's Advanced Audio Codec (AAC), etc.

To provide a comprehensive disclosure without unduly lengthening the present specification, applicants incorporate by reference the patent publications and applications cited herein.

We claim as our invention all such embodiments as may come within the scope and spirit of the following claims, and equivalents thereto:

1. A method comprising:

presenting a digitally encoded object to an optical sensor, the optical sensor producing output data;

decoding plural-bit data from the sensor output data; and

using said plural-bit data to establish a link to an internet address having data relating to said object;

wherein the object is steganographically encoded with said plural-bit data.

2. The method of claim **1** in which the object is a business card.

3. The method of claim **1** in which the object comprises printed advertising.

4. The method of claim **1** in which the object comprises product packaging.

5. The method of claim **4** in which the product packaging comprises a cover associated with packaged music media.

6. The method of claim **1** in which the object comprises a portion of a book.

7. The method of claim **1** in which the object comprises an article of postal mail.

8. The method of claim **1** in which the object comprises printed advertising.

9. The method of claim **1** in which the plural-bit data comprises a code, the method including consulting a data

structure to obtain an internet address associated with the code, and initiating a link to said address.

10. A method of initiating access to a computer via a data communications medium, the method comprising:

receiving data corresponding to an object, said object comprising visual data and having information indicative of an address associated with the computer steganographically embedded in-band within said visual data;

decoding the information from said object; and

initiating a link to the computer using said information;

said decoding and initiating being performed by the same device.

11. The method of claim **10** in which said receiving comprises receiving said object from a digital storage or transmission medium in digital form, without said object having being rendered in human-perceptible form since being steganographically embedded.

12. The method of claim **10** in which said receiving comprises sensing a human-perceptible form of said object, as by an optical sensor device.

13. A method of initiating access to a computer via a data communications medium, the method comprising:

receiving data corresponding to an object, said object comprising visual data and having information indicative of an address associated with the computer steganographically embedded in-band within said visual data;

decoding the information from said object; and

initiating a link to the computer using said information;

wherein said receiving comprises receiving said object from a digital storage or transmission medium in digital form, without said object having being rendered in human-perceptible form since being steganographically embedded.

14. A method of initiating access to a computer via a data communications medium, the method comprising:

receiving data corresponding to an object, said object comprising visual data and having information indicative of an address associated with the computer steganographically embedded in-band within said visual data;

decoding the information from said object; and

initiating a link to the computer using said information;

wherein said visual data includes plural samples, said steganographically embedded information extending generally throughout said samples, rather than localized in one or more particular portions thereof, wherein the information can be decoded from an excerpt of said visual object and used to initiate the link to the computer.

15. A method of initiating access to a computer via a data communications medium, the method comprising:

receiving image data corresponding to a printed object, the printed object including both text and background, at least the background having information indicative of an address associated with the computer steganographically embedded therein;

decoding the information from said image data; and

initiating a link to the computer using said information.

16. The method of claim **15** in which said information comprises a code, the method including consulting a database to obtain a computer address associated with said code, and initiating a link to said address.

17. The method of claim **15** in which the printed object comprises a business card.

18. The method of claim **15** in which the printed object comprises printed advertising.

19. The method of claim **15** in which the printed object comprises product packaging.

20. The method of claim **15** in which the product packaging comprises a cover associated with packaged music media.

21. The method of claim **15** in which the printed object comprises a portion of a book.

22. The method of claim **15** in which the printed object comprises an article of postal mail.

23. The method of claim **15** in which the printed object comprises printed advertising.

* * * * *

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 6,311,214 B1
DATED : October 30, 2001
INVENTOR(S) : Geoffrey B. Rhoads

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page,
Item [63], change "which is" to -- and --, after "Apr. 15, 1999" add -- which claims priority to application 60/082,228, filed on April 16, 1998 --.

Column 7,
Line 35, change "data The" to -- data. The --.

Column 19,
Line 34, change "comers" to -- corners --.

Column 52,
Line 38, change "samples pixels)" to -- samples (pixels) --.

Column 57,
Line 1, change "desired In" to -- desired. In --.

Column 58,
Line 11, change "entirely" to -- entirety --.

Column 61,
Line 61, change "watermark In the" to -- watermark. In the --.

Column 63,
Line 5, change "watermark The presence" to -- watermark. The presence --.

Signed and Sealed this

Ninth Day of September, 2003

JAMES E. ROGAN
Director of the United States Patent and Trademark Office

US006297819B1

(12) **United States Patent**
Furst

(10) **Patent No.: US 6,297,819 B1**
(45) **Date of Patent: Oct. 2, 2001**

(54) **PARALLEL WEB SITES**

(75) Inventor: **Merrick L. Furst**, Pittsburgh, PA (US)

(73) Assignee: **Essential Surfing Gear, Inc.**, Pittsburgh, PA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/192,633**

(22) Filed: **Nov. 16, 1998**

(51) **Int. Cl.**[7] **G06F 3/00**

(52) **U.S. Cl.** **345/329**; 345/346; 707/501; 707/513; 709/203

(58) **Field of Search** 709/201, 203; 345/329, 346; 707/501, 513; 395/200.33, 200.49

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,625,781	*	4/1997	Cline et al.	345/335
5,649,186	*	7/1997	Ferguson	707/10
5,794,230	*	8/1998	Horadan et al.	707/2
5,796,393	*	8/1998	MacNaughton et al.	345/329
5,801,702	*	9/1998	Dolan et al.	345/357
5,809,248	*	9/1998	Vidovic	709/219
5,854,630		12/1998	Nielsen	345/352
5,970,064		10/1999	Clark	370/351
5,974,446	*	10/1999	Sonnenreich et al.	709/204
6,018,344	*	1/2000	Harada et al.	345/357
6,031,528		2/2000	Langfahl	345/334
6,032,162		2/2000	Burke	707/501

OTHER PUBLICATIONS

International Search Report mailed Sep. 8, 2000 in PCT/US99/27159 (related PCT application).*

Asnicar, F.A., and Tasso, C., "ifWeb: a Prototype of User Model–Based Intelligent Agent for Document Filtering and Navigation in the World Wide Web", Proceedings of the workshop "Adaptive Systems and User Modeling on the World Wide Web", Sixth International Conference on User Modeling, Chia Laguna, Sardinia, 2–5 Jun. 1997.*

Alexa Internet Tour, 1 pg., downloaded from www.alexa-.comwhatisalexa/index.html, Jan. 1999.

"Revolutionary Ad Model," Advertise on Alexa, 1 pg., downloaded from www.alexa.com/company/advertise.html, Jan. 1999.

"The Alexa Service appears on your desktop in its own window," 1 pg., downloaded from www.alexa.com/tour/overview.html, Jan. 1999.

"Know more about the sites you visit," 1 pg., downloaded from www.alexa.com/tour/site_stats.html, Jan. 1999.

"Find Related Web Sites," 1 pg., downloaded from www.alexa.com/tour/related_Links.html, Jan. 1999.

"500,000 Sites and Growing," 1 pg., downloaded from www.alexa.com/tour/archive.html, Jan. 1999.

"Research Tools at Your Fingertips," 1 pg., downloaded from www.alexa.com/tour/eb.html, Jan. 1999.

"Reporting," 1 pg., downloaded from www.alexa.com/company/reporting.html, Jan. 1999.

"Alexa Internet's Related Links Integrated into Netscape Browsers," 1 pg., downloaded from www.alexa.com/company/netscape.html, Jan. 1999.

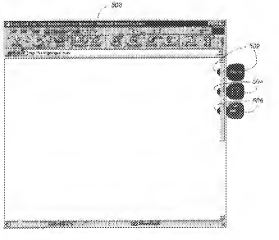
(List continued on next page.)

Primary Examiner—Raymond J. Bayerl
Assistant Examiner—Cuong T. Thai
(74) *Attorney, Agent, or Firm*—Fish & Richardson P.C.

(57) **ABSTRACT**

Systems, methods, and apparatus (including computer program apparatus) for a browser-aware application delivery system. The System provides World Wide Web browser extensions based on server processes rather than on plug-in program modules loaded and installed on a user's machine. The system operates like a monitor for a user while the user is browsing the web, and enables the user to obtain and interact with context-sensitive services and information based on the user's browsing activity. The system allows the user to add application tools, which are implemented on servers separate from the user's computer. Third parties can easily add tools to the system by registering application services with the system.

28 Claims, 5 Drawing Sheets



OTHER PUBLICATIONS

"Demographics," 1 pg., downloaded from www.alexa.com/company/demographics.html, Jan. 1999.
"Ads appear in the pop–up and on the bar," 1 pg., downloaded from www.alexa.com/company/adspecs.html, Jan. 1999.
Alexa Why Crawl, 1 pg., downloaded from www.alexa.com/support/why_crawl.html, Jan. 1999.
GIF image 590x329 pixels, Alexa, 1 pg., downloaded from www.alexa.com/tour/images/alexa_overview.gif, Jan. 1999.
"It's X–treme!", Alexa, PC Magazine: The Best of 1998, 1 pg., downloaded from www.zdnet.com/pcmag/special/bestof98/internet5.html, Jan. 1999.
"Search While You Surf," PC Magazine: Search the Web, 1 pg., downloaded from www.zdnet.com/pcmag/features/websearch98/surf.html, Jan. 1999.
Alexa 1.4.1 Support Pages, 9 pgs., downloaded from www.alexa.com/support/index 1.html, Jan. 1999.
Alexa General FAQs, 4 pgs., downloaded from www.alexa-.com/whatisalexa/faq.html#general, Jan. 1999.
"Custom Explorer Bars Give Sites an Edge," 2pgs., downloaded from www.microsoft.com/Windows/Ie/IE5/custom-.asp, Jan. 1999.
"Flexibility Across the Web," 2 pgs., downloaded from www.microsoft.com/Windows/Ie/IE5/choice.asp, Jan. 1999.
"Web Accessories Overview," 2 pgs., downloaded from www.microsoft.com/workshop/ . . . er/accessory/overview/overview.asp, Jan. 1999.
Alexa Technology, 4 pgs., downloaded from www.alexa-.com/support/technology.html, Jan. 1999.
"Browser Extensions Overview," 2 pgs. downloaded from www.microsoft.com/workshop/browser/ext/overview/overview.asp, Jan. 1999.
"Creating Custom Explorer Bars and Desk Bands," 13 pgs., downloaded from www.microsoft.com/workshop/browser/ext/overview/Bands.asp, Jan. 1999.

* cited by examiner

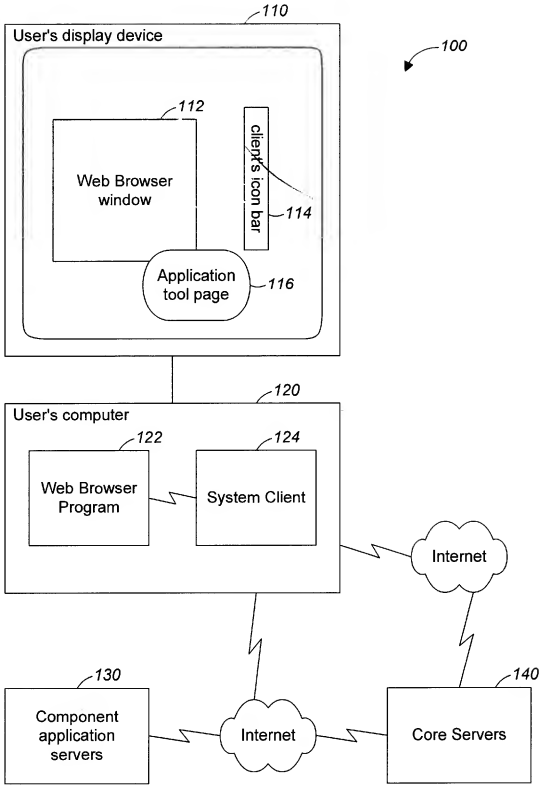

110
User's display device
100
112
Web Browser window
client's icon bar
114
Application tool page
116
120
User's computer
122
Web Browser Program
124
System Client
Internet
130
Component application servers
Internet
140
Core Servers

FIG. 1

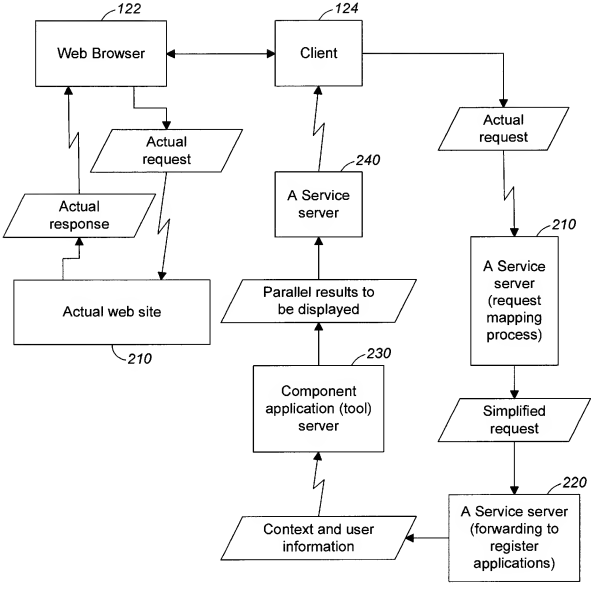

122
Web Browser
124
Client
Actual request
Actual response
Actual request
240
A Service server
210
A Service server (request mapping process)
Actual web site
Parallel results to be displayed
210
230
Component application (tool) server
Simplified request
220
Context and user information
A Service server (forwarding to register applications)

FIG. 2

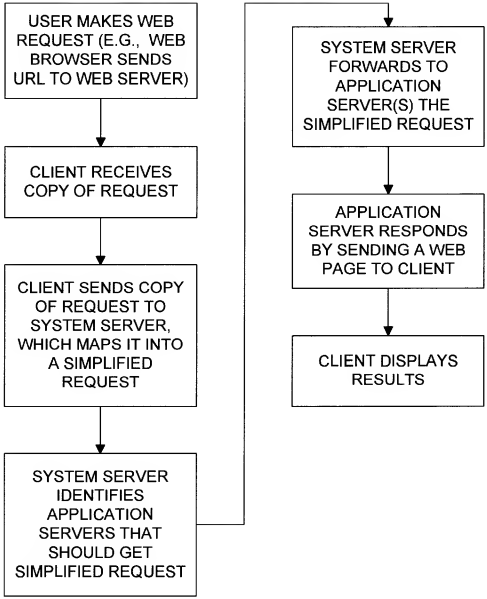

USER MAKES WEB REQUEST (E.G., WEB BROWSER SENDS URL TO WEB SERVER)
CLIENT RECEIVES COPY OF REQUEST
CLIENT SENDS COPY OF REQUEST TO SYSTEM SERVER, WHICH MAPS IT INTO A SIMPLIFIED REQUEST
SYSTEM SERVER IDENTIFIES APPLICATION SERVERS THAT SHOULD GET SIMPLIFIED REQUEST
SYSTEM SERVER FORWARDS TO APPLICATION SERVER(S) THE SIMPLIFIED REQUEST
APPLICATION SERVER RESPONDS BY SENDING A WEB PAGE TO CLIENT
CLIENT DISPLAYS RESULTS

FIG. 3

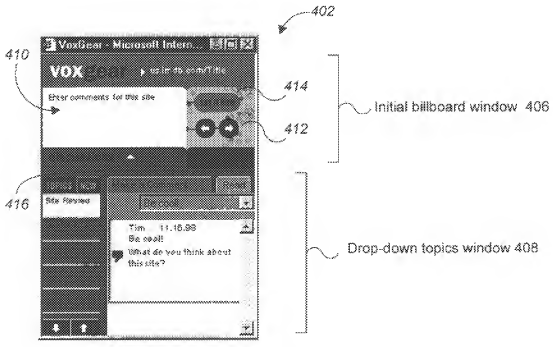

402
410
VoxGear - Microsoft Intern...
VOX
Enter comments for this site
414
412
Initial billboard window 406
416
Site Revised
Report
Tim 11.16.98
Be cool!
What do you think about this site?
Drop-down topics window 408

FIG. 4A

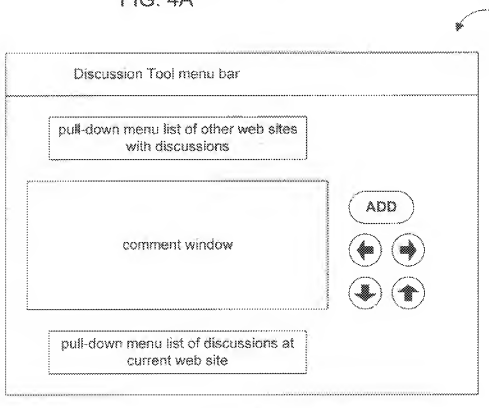

404
Discussion Tool menu bar
pull-down menu list of other web sites with discussions
comment window
ADD
pull-down menu list of discussions at current web site

FIG. 4B

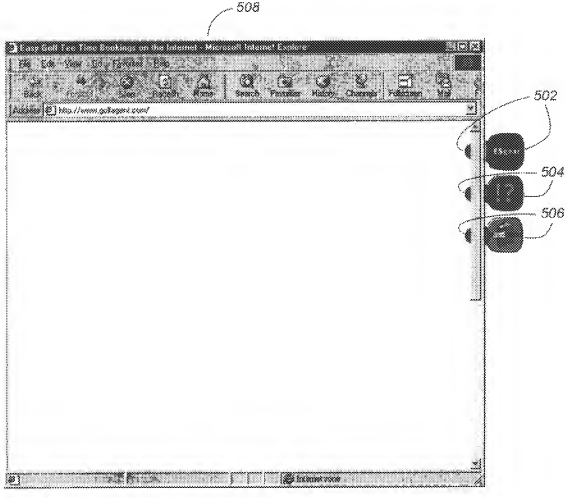


FIG. 5

PARALLEL WEB SITES

BACKGROUND OF THE INVENTION

The present invention relates to programs and systems that enable a user to interact with sites on a network, such as World Wide Web sites on the Internet.

The term World Wide Web (the "WWW" or the "web") is used variously to refer to (i) protocols that facilitate access to data through a web browser program presenting a graphical user interface to its user, or (ii) the set of pages that a user can access using such a web browser over the Internet. A web page will generally contain references to related material that are presented as links. By selecting (i.e., opening) a link, a user can access the referenced material. Using links, users can jump from one document (web page) to another, a process called browsing. The architecture of the web that provides these features has three parts: the server, which provides the information source, the browser, which takes the information and formats it in a particular way, and the network which provides the communication between the two.

Web pages are electronic documents are encoded in compliance with a HyperText Markup Language ("HTML") standard. HTML standards are generally promulgated by the World Wide Web Consortium (W3C), although some companies have promulgated their own extensions and versions. Background and current information about HTML can be found on the web site of the World Wide Web Consortium, whose URL is http://www.w3.org. HTML documents in the web context are generally referred to as pages or web pages. Web pages are text files containing content text (i.e., the information to be displayed to a user) and HTML instructions. Programs referred to as browsers (or, if needed for clarity, web browsers)—such Netscape Navigator, NCSA Mosaic, Lynx, and Microsoft Internet Explorer—are computer program applications that interpret the HTML instructions in an HTML document and, in accordance with the instructions, display the document's content to the user.

Links are HTMI instructions used within web pages to identify or locate hypertext elements, such as images, sounds, locations within the current web page, or other web pages. A reference to a web pages is generally a URL (a Uniform Resource Locator), which contains sufficient information to allow a web browser, interacting with a web server, to obtain the specific web page. Links are often displayed graphically on a displayed web page by text of a particular format or by a clickable icons. When the browser opens a link, the browser initiates a network connection (if necessary) to obtain the referenced element, which the browser then displays or plays, according to the nature of the element.

SUMMARY OF THE INVENTION

The invention provides systems, methods, and apparatus (including computer program apparatus) that implement and constitute aspects of a browser-aware application delivery system (which will be referred to as the "System") and of a service based on the System (the "Service"). The System provides browser extensions that are based on server processes rather than on plug-in programs, such as Netscape plug-ins or Microsoft ActiveX controls, that have to be loaded and installed on the user's machine. The System operates like a monitor for a user while the user is browsing the web, and enables the user to obtain and interact with context-sensitive services and information based on the user's browsing activity. The context is defined at least in part by what web page the user is viewing or requesting, and it is optionally defined by requests (such as search requests or the actual URL) made by the user to a site or by a history of sites visited and requests made.

In one implementation, the System includes a core of functionality to which can be added user-selectable component application tools and services. The application-specific services of the component applications tools (which may be referred to as component applications, application tools, applications, or simply as tools) are provided by an application server, which is a server process running on one or more dedicated or shared computers connected to the System, generally through a network connection. The core functionality is provided by one or more servers, which for that reason may be referred to as core servers, and a client program running on the user's computer that interacts with the user's running web browser and with the core servers. The client program of the System (which will generally be referred to simply as the "client") runs on a user's computer and receives information about what the user is doing on the web from the user's web browser. The user can easily select and enable component application tools, whose functionality becomes available to the user through the client icons and windows. Enabled applications can and generally will present an application icon through a graphical user interface maintained by the client, and application services will generally be presented through an application tool home page and other web pages generated by an application server and displayed by a web browser operating as a program embedded in the client.

Advantages that can be seen in implementations of the invention include one or more of the following.

The System and its components are useful to users ranging from casual to serious web surfers. The System enhances the user's web surfing experience for entertainment, community-building, transaction support, and knowledge acquisition.

The value of the System to its users increases with the number of users and the number of available applications. Third-party vendors can develop and distribute component applications to users. Such component applications can provide value for the user and increased revenue for the third-party vendors. The development and distribution of applications for the System can be done in collaboration with, or independently of, the provider of core System services.

The System provides value to a user in the cumulative value of all the available application tools. Component application tools are easy to find and install. The System operates transparently as the user browses the web. When it is not actively in use, the System does not inhibit the user's web surfing environment by slowing it down, taking up too much screen real estate, or otherwise.

The System allows component application suppliers to provide supplementary value to users as the users surf the web. The System appears to travel with the user as the user browses the web. This enables the user to find at every web site additional functionality that is independent of the web site. The content served when a user visits a web site can be contextually-specific and therefore relevant to the exact web site being viewed.

The set of core servers is readily scalable to handle large numbers of active users.

Component applications can have distinct advantages over applications based at web sites. The information accessed through component applications is independent of

any particular web site context both in location and in point of view. The information is contextual so a user gets information about what the user is immediately interested in. The System can be customized for each user. Users can choose to select and enable only the component applications they find useful.

The System enables sales and marketing efforts to be brought to the context of a user-selected web site, so users can find the goods and services that they might be seeking in the context in which they are currently browsing. The System brings the added value to electronic commerce of enabling the right transaction by making the user better informed. A user can augment his or her range of choice by selecting which contextual sales applications are valuable enough to warrant installation and use.

The System can be used to provide contextual sales applications as component applications having a standard form of presentation and interaction. As a consequence, transactions made using such contextual sales applications can be faster for the user than conventional web site transactions because the use of a standard interface means the user does not have to relearn the purchasing process with each new web site the user visits.

In addition, component sales applications can provide a bidirectional flow of information. That is, dialog and information can flow to inform the seller of the buyer's needs and preference, or to allow multiple buyers to share information about products and services. Such bidirectional flow provides independence and ability for dialog that helps a consumer make an informed decision.

To the provider of a contextual sales application, such an application can provide data on users' patterns of use, behavior, and purchasing; and this data can be provided in real time. For example, when a user arrives at a bookseller's site, the bookseller's contextual sales application can inform the site of the web sites that were just visited by the user. In addition, the application can detect that the user has performed a search at another web site and then deliver to that user a list of books on related topics and let the application's site know where the user is.

An Internet portal, by offering component applications, not only can interact with a user at the portal site but also can travel with the user, providing additional services as the user surfs other web sites. The use of traveling component applications counters the portals' disadvantage that users leave once they have what they came to the portal for. It also allows a portal to provide context-sensitive value to the users all over the web, even users who do not come to the portal's own web site.

The System enables users to communicate with other web site visitors in a context directly relevant to whatever site the user is visiting. The System permits the posting and viewing of data relevant to a web page without the consent and/or moderation of the web site owner. The user can have access to information and services related to, but independent of the control of, the web site the user is visiting. Use of the System can thus create, and enables users to reach, situated communities and knowledge. For example, the System enables organizations to create and host members-only discussions areas at sites that may be visited by their members.

The details of one or more embodiments of the invention are set forth in the accompanying drawings and the description below. Other features and advantages of the invention will become apparent from the description, the drawings, and the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. **1** is a schematic block diagram of the architecture of an implementation of the System of the invention.

FIG. **2** is an elaboration of the block diagram of FIG. **1**, further illustrating a flow of information in accordance with the invention.

FIG. **3** is a flowchart illustrating a flow of operations of the System in accordance with the invention.

FIG. **4**A and FIG. **4**B are each a diagram of a user interface window of a discussion tool of the System.

FIG. **5** is illustrates a web browser window displayed with component application tool icons in accordance with the invention.

Like reference numbers and designations in the various drawings indicate like elements.

DETAILED DESCRIPTION

As shown in FIG. **1**, an implementation **100** of the System includes a user's computer **120** configured with a web browser program **122**, such as Microsoft® Internet Explorer version 4.01 (which supports DHTML) in the illustrative implementation, and a System client program **124**, which will be described.

As is well known, the web browser operates to display, in response to user input, web pages in one or more windows **112** on a display device **110** coupled to the user's computer **120**. The client **124** operates to display a graphical user interface **114**. In the illustrative implementation, the user interface **114** takes the form of an icon bar, and so will be referred to as the bar. The bar is the user's interface to the System and, after the client software has been installed and the System has been enabled by the user, the bar is always visible to the user while the user is browsing the web. On the bar, the System and any component applications enabled by the user are represented as one or more icons or buttons. A logo icon on the bar represents the System itself. The logo functions as a menu button. When it is activated, by a mouse click, for example, an options menu for System functions is displayed.

The client also operates to display web pages created by or for component application tools in windows **116** on the display device **110**.

To interact with, and receive the services of, the System, a user must install the client software and register with the System. The client software is delivered to, and installed on, the user computer by a conventional web browser download and installation process.

Users who have registered may be referred to as members or registered members to emphasize that they are known to the System. Each member has a screen name and a unique user identifier ("user ID"). A profile is created and stored on a System database for each member at registration. A profile contains the following fields: a System-assigned user ID, a user-selected screen name, and an e-mail address for the user. A profile may also contain additional information such as gender, age, and occupation. Members can access their profiles by clicking on a profile link on the options menu.

In registering a user, the System sends to the user's computer a cookie that holds the user's identity. When the client **124** is launched, either automatically when the user launches the web browser **112** or otherwise, the client sends the cookie to the a System server to initiate a connection with the System.

The client **124** is essentially a thin shell for an embedded web browser, whose function is to display web pages sent by the System or by component application tools. The System and its component tools operate to create a web pages that parallel or shadow actual web pages (that is, web pages that

exist outside and independent of the System and its tools). Parallel pages are implemented in JScript and DHTML (Dynamic HTML). In the particular implementation being described, the version of DHTML used is that defined for the Microsoft® Internet Explorer 4.01 web browser ("IE4"). The client **124** embeds a Microsoft® WebBrowser control to implement web browsing and display functionality in the client. In particular, this control provides the DHTML functionality of binding data, such as a database or a comma-delimited file, to HTML tables or other HTML elements on a loaded parallel page.

The client **124** communicates with the web browser **122** through a set of Microsoft® application program interfaces (APIs), specifically DWebBrowserEvents2 to listen to IE4, and IWebBrowser2, IHTMLElement, IHTMLDocument2, and IHTMLWindow2 to control and query IE4. As part of the installation and registration process, the client is registered with the web browsers, so that when the user launches the web browser **122**, the web browser causes the client **122** to be launched automatically.

The core servers **140** are a collection of computer program processes and digital data running and stored on one or more computers in one or more locations. In the illustrative implementation, the administrative, communications, and application support functionality is distributed among programs, databases, and computers in a conventional way. More particularly, the server environment has two classes of computers: communication servers and database servers. The servers are high-end Sun™ servers configured to support performance, scaling, and security. The operating system for all servers is Sun Solaris 2.6. The servers run AOL server™ 2.3. Database servers run Oracle™ RDBMS. All data is stored on database servers. Only HTML cookies are placed on the user's computer.

The application servers **130** can be implemented on any hardware and software platform that is sufficient to support the communications, data storage, and application service requirements of the particular application tool provided by the respective server.

As shown in FIG. **2**, the web browser and client exchange data with each other as has been described. As the user is browsing the web, the client listens to the browsing requests made by the user. In the present implementation, the client receives the URLs that the web browser sends to an actual web site **210**, regardless of how they are generated. URLs can be generated by clicking on or otherwise opening a link, by typing a URL into a dialog, or by a web page in response to a search request or other action of filling in a form.

Under certain circumstances, the clients stops listening to the web browser. For example, for security reasons, the client stops listening when a secure connection is being made with the HTTPS (HyperText Transmission Protocol, Secure), a URL access method for connecting to HTTP servers using SSL (Secure Sockets Layer), or if the target of the request is local file storage, such as a disk volume on the user's computer. For considerations of performance, the client stops listening if the protocol is not HTTP (HyperText Transmission Protocol) or FTP (File Transfer Protocol), or if the target of the request is local file storage, such as a disk volume on the user's computer.

Having heard a request, the client transmits a copy of the request to a System server **210**. This server performs a mapping process that produces a simplified request **128** for further processing. Operating on URLs, this mapping process produces simplified URLs from actual URLs. The mapping process applies to an actual URL a list of rules to find a first match. In the present implementation, the rules are expressed as regular expressions. The first match defines the mapping. The mapping can be a many-to-one or one-to-one mapping of any kind, because the simplified URLs need not be valid—that is, the simplified URL need not actually specify the location of an object. For example, a mapping may be a transformation of the actual URL (for example, one that strips trailing characters) or a fixed mapping to a particular simplified URL. By using simplified URLs, the System can capture the essence of what the user is browsing with his or her actual requests.

The regular expressions are built by hand based on an analysis of actual URLs. The analysis is supported by a URL maintenance spider, which is a subsystem that tests all of rules by applying them to the universe of actual URLs that the System has seen and determines whether all of the simplified URLs known to the System are generated by the rules. Any simplified URL that is not generated by application of some rule is an orphan. The maintenance spider generates a list of orphans so that the rules can be revised as necessary. This testing is done whenever the rules are changed.

The following two examples illustrate such rules.

First, the following two lines say to map any URL ending in /index.htm or /index.html to one that ends in/.

```
/index\.html?$
/
```

With this rule,

http://www.mathcs.duq.edu/~jackson/index.html

maps to

http://www.mathcs.duq.edu/~jackson/.

Second, the following two lines say to map any URL at www.amazon.com and containing a field consisting of digits and dashes to a URL with the digit-and-dash field and everything following it stripped off.

```
^http://www\.amazon\.com/(.*)/([0-9]+)-)+[0-9]*(/$)(.*)
http://www.amazon.com/\1
```

With this rule,

http://www.amazon.com/exec/obidos/subst/home/home.html/002-6380188-9496641

maps to

http://www.amazon.corn/exec/obidos/subst/home/home.html

Having a simplified URL **128**, a forwarding process **220** of the System forwards the simplified URL to those applications that have registered an interest in the simplified URL. When an application is installed or registered as a component application tool of the System, the application identifies for the System those simplified URLs that the application is interested in seeing, that is, under what circumstances the application wishes to be notified of the user's browsing activity. The notification conditions can include one or more of the following, which can be applied in combination: notify the application when the user opens an actual page that includes one of a list of keywords; notify the application when the user opens a page with a simplified URL matching a list of URLs or a list of regular expressions; notify the application when the user clicks on the application's icon on the bar; or notify the application when the user's context changes if the user has an application window

open in the client. If any of the notification conditions apply, the context and user information are sent to the application server **230**. The context can include, in addition to the current simplified URL (request), the actual URL (request), the matching keyword if a keyword match was satisfied, and a history of preceding simplified or actual URLs (requests), or both, if requested by the application.

The application server **230** includes an application process that receives the user and context information, and computes a reaction, which will in general be a web page to be displayed by the web browser embedded in the client. The application server transmits the reaction to a System server **240** (which may but need not be implemented on a computer different from servers **210** or **220**) for formatting and transmission as a parallel web page to the user's client. Alternatively, the application server can transmit a reaction page to the user's client directly. If the user does not have a client browser window open for the application, the application will generally send a web page to animate the application's icon on the user's bar in some way, to let the user know that the application may have something of interest for the user in the current context. The user then clicks on the application icon in the bar to open a browser window with a web page provided by the application server. Animation can include one or more of lighting up the icon, changing the colors of the icon, producing sound, or producing movement such as rotation.

Because evaluating context-specific notification conditions (either in the application server or in a core server) is expensive, many applications will remain dormant for a user until the user opens the application by clicking on the application's icon on the bar. The System notifies the application server, which responds with a web page for a client browser window.

FIG. **3** is a flowchart of the process that has just been described.

The architecture of the System allows third parties to add new applications easily. Using the basic functionality of the System, a third party registers a new tool with the System by providing to the System a registration link to a registration page, which will generally be on a third-party server. The registration link can be provided using HTTP or some other protocol, such as HTTPS, for example by submitting a URL with an embedded URL for the registration link. The registration page contains the following items, or links to the following items: a tool icon to be displayed by the client on the bar; (optional) an animated tool icon to be displayed by the client on the bar; a link to be opened when user activity of interest to the tool occurs; and (optional) the conditions under which the tool is to be notified. The default notification condition is that tool is notified when the user has an enabled the tool (e.g., by clicking on the tool icon on the bar) and the web browser context changes. When that occurs, a notification is sent to the tool through the link provided at tool registration. Thus, simply by providing an icon and what amounts to a call-back address, the third party can register its tool with the System and begin operation.

When a notification is received by the tool, the tool must determine how to respond. In general, the tool will provide a reaction such as displayable output in HTML or DHMTL to a System core server, which then packages the reaction as necessary and forward it to the user's client for display. The client browser (that is, the web browser embedded in the client) generally maintains at least one client browser window for each active (that is, open) tool. If browser display is received by the client from a tool, the client will open a client browser window for the tool, if one is not open already. The tool can optionally specify content for more than one client browser window, in response to which the core server will cause the client to display the required windows.

As with any other browser window, the client browser window can be used to display web pages with links that the user can open, with the possible consequence that further client browser windows will be opened. This navigation and browsing through the client windows will be unaffected by the System until the user browses in a web browser window, which in general will cause the context to change. In general, when the context changes, the tool will transmit a reaction that will result in a display in a client browser window that displaces whatever had been displayed there.

The user can have any number of tools active (i.e., open) at one time. As the user navigates the web using the web browser and the context changes, the client tool windows of all the active tools will be updated by the tools with information generated by (or at the request of) the application programs running on the tool servers.

The client browser windows and bar can be positioned by the user. Optionally, the client can position its windows and bar itself, in effect attaching them to the current web browser window by calculating their location relative to the current web browser window and moving them when the current web browser window moves. In this way, the client can create the appearance that the icons of the bar are attached to web browser window. Generally, in implementing this option, the bar will be placed so as not to overlap the web browser window; however, when the window is so large or positioned in such a way that this is not possible, then the client moves the bar into the web browser window to the extent necessary. In a further alternative implementation, the user can position the client windows and bar relative to the current web browser window (rather than relative to the display co-ordinates). If options are implemented, the user can select a positioning option from the System logo options menu.

It should be noted that while the user interface elements of the client have been referred to as windows and a bar, these elements can take other forms, including free-form graphics displayed without enclosing boxes or window decorations. For example, the bar icons can be visually noncontiguous, as are the two-part illustrative icons **502**, **504**, and **506** in FIG. **5**, which appear to span the scroll bar of the current web browser window **508**.

Discussion Tool

The features and advantages of the System can be appreciated from a description of an implementation of a particular component application, the discussion tool.

As has been described generally, operation of the discussion tool includes program and data components residing on a core server computer and on a discussion tool application server computer, which may be the same or a different computer. The client transmits the user's web browsing activity to the core server. The core server maps each actual URL received from the client to a simplified URL, as has been described. If the discussion tool has been enabled by the user, i.e., if the discussion tool icon is on the bar, the simplified URL, which defines the current context, and the user ID is supplied to the discussion tool server. The discussion tool server determines whether a discussion parallel to the site represented by the simplified URL exists. If such a discussion exists, the server animates the discussion tool icon on the bar. This alerts the user to the existence of a discussion that may be of interest.

A discussion is a collection of individual comments, generally organized under one topic. A comment is an individual message a member can create, post and read in the context of a web site. Comments are organized by topic into discussions. Discussions have an author, the person who created the discussion; a topic, a category or title of a discussion; and, optionally, an expiration, an amount of time before discussion will expire.

When the user selects the discussion tool icon—in response to animation or otherwise—a discussion tool window **402** or **404** appears, as illustrated in FIG. **4**A and FIG. **4**B, respectively. The discussion tool user interface is defined by a discussion tool home page, which is displayed in a client discussion tool window by the client's embedded browser. Because the discussion tool user interface is defined by a web page, the user interface for the discussion tool can take a wide variety of forms.

In one implementation, the discussion tool initially opens a small window **406** that has a comments area **410** for the billboard. The billboard is the general discussion for each context. It exists without a user creating it, and it does not expire. The comments area **410** can be used for both the entry and display of general discussion comments, navigation buttons **412**, and other controls, such as a say-it control **414** to speak the current comment. The controls can also include a quick-reply button that allows users to reply quickly to the general discussion, and a tell-a-friend button that allows users to invite friends to the general discussion. The comments area **410** shows recent comments from the general discussion.

The initial window **406** has a discussions-at-site button **416** to open up to a window or pane **408** showing the named discussions associated with the context. The user can see more named discussions by opening the bottom portion of the window. There the user can scroll through existing topics and read or add comments, add a new topic, and invite others to view the discussion. If no discussions exist for the context, the user can initiate a discussion.

The data model of the discussion tool includes, among others, the following elements: discussion, general discussion, comment, vote comment, invitation, a user interface, a parallel page corresponding to each simplified URL, profile, screen name and user ID, flag notification, expiration meter, subscription, digest, my-subscriptions page, private discussions, and permissions. Discussion and general discussion have already been described.

The expiration time of a discussion can be displayed on a meter or as a text message. Members can prevent expiration by adding to the amount of time left in some way through the user interface. An expiration meter is a graphic that is displayed beside the discussion topic. It reflects the amount of time a discussion has before it expires. A member can click on a button to extend the life of a discussion. The System can optionally set a maximum life of a discussion.

A vote is a special type of comment that invites a set of users to participate in a limited tally or poll. Creating a vote involves writing a question with two or more resolutions. The question is displayed and participating members can select from the resolutions and cast their vote. The discussion tool tabulates votes and displays the results through the discussion user interface. The user creating the vote can elect to limit display to the invited participants.

An invitation is an e-mail message inviting the recipient to visit a web site and/or participate in a discussion at a web site. In creating an invitation, the discussion tool includes in the message a dynamic link (such as a URL) to the web site and discussion from which the invitation was sent. An invitation can contain a custom message from the user sending the invitation. When a member sends an invitation, the System checks to see if the recipient is also a member, that is, if the recipient is known to the System. If the recipient is a member, the invitation is sent with a link to the discussion. Otherwise, the System first directs the recipient to a core server web site to download and install the client software, get a user ID, and register a screen name. The recipient can then go back to the invitation and click on the link to the discussion to which he or she was originally invited.

A private discussion is a discussion created by a member with a list of participants. Only members on the participants list will see the private discussion or even know it exists. The author member can give or deny other participants permission to add new participants to the list.

A moderated discussion is one that is hosted, by a sponsor of a web site, for example. A moderated discussion has a moderator who can edit the content the discussion.

A subscription is a way for a user to follow a discussion. When a user subscribes to a discussion, the user receives a digest of activity within the discussion. Discussions to which a user is subscribed are indicated on the discussion tool topics panc **408**. The discussion tool window optionally has a control, such as a button, to allow a member to subscribe or unsubscribe to a particular discussion.

A digest is an e-mail summary of activity on a discussion to which a user has subscribed. It includes a link to the discussion. It is sent by e-mail on a regular basis, which the user can select. It is sent only if there is activity on the discussion. It contains the discussion title, discussion URL, discussion expiration (or time left), and all comments since the last time a digest was sent to the user or since the subscription was requested.

The my-subscriptions page is a list of all subscriptions to which a user has subscribed. It provides URL links to subscribed discussions, allows the user to unsubscribe, allows the user to control digest frequency, and allows the user to edit the user's e-mail address.

The discussion tool uses a number of subsystems. The discussion expirer subsystem controls expiration of discussions in the discussion database. It runs queries on the database to find discussions that are ready for expiration and deletes them from the database. It is a constant parameter file, editable to control the frequency of queries to the database. It can be accessed from the administrator pages.

The bounce handler subsystem handles e-mail messages bounced back to the System. The invitation subsystem generates e-mail invitations with URL links. And the digester subsystem generates timed digests and subscriptions.

Other Component Application Tools

As has been mentioned, the System enables and can support many different kinds of applications. One useful kind of component application is the contextual sales application.

Contextual sales applications can be developed and offered by third-parties independent of the provider of the Service to promote contextual sales to users. For example, a third-party organization can offer its point of view relative to the sites being browsed, alert the user to organization-sponsored member discounts at travel web sites, or provide the organization's point-of-view commentary on issue-

oriented or news sites, and so on. As a second example, a bookseller can allow the user to view a list of links to specific books on topics that are directly relevant to the web page or site the user is currently viewing, or to the sequence of pages or sites the user has been viewing, and to offer competitive pricing, coupons, discounts, one-click buying, and so on.

The main perceived difference between contextual sales applications and other types of application is that contextual sales applications are used for transactions, and so users expect that transactions that they make using contextual sales applications will be secure and confidential. This feature is provided because the client supports HTTPS communication.

Because the architecture of the System is open, many kinds of component applications can be developed and distributed easily. The following examples illustrate the variety of applications that can be supported.

A school application tool offers students and faculty access to, or commentary on, specific web sites that are used for research, information or projects. When the tool is opened, a client tool window appears with controls allowing the user to add the context (i.e., the current web browser site) to the set of sites accessible through the tool, to add comments to the tool's database of comments on the context, to display the set of sites and navigate the web browser to one of the sites by selecting it in the client window.

A graphic application tool allows users to spray paint or doodle electronically on web sites and to post their own graffiti and selectively view other users' posted works. The tool's client graffiti window for drawing is drawn as a graphic with no box or decoration, and it is positioned relative to, and therefore appears to be attached to, the web browser window displaying the context site. The graffiti window acts like a transparent layer over the site.

A coding application tool allows programmers to translate source code, edit it and view results, explain odd instances of HTML code used on various web pages, deconstruct and explain construction of elements on a page. The tool server receives the actual context URL, which it uses to obtain the source code of the site the user is browsing. The tool displays the source code in a client browser source code window and the interpreted source code in a client browser document window. The tool synchronizes the display of the interpreted source code window and the document window so the user can see the corresponding views of source code and results. The user can select cursor tools from a pop-up context menu to edit the source code and request help windows for selected features.

A company information application tool displays a hierarchy of information about a particular company whose web site the user is viewing without requiring the user to navigate to other web sites to look it up.

A click-and-close application tool receives information about the user from the user in a fill-in form and stores the information in a database, optionally under password protection. When the tool is then activated from the icon bar in a context that includes a fill-in web-based form, the tool autofills form with the information, which makes filling out order or application forms faster for the user and more consistent. If the context form requires information the tool does not have, it requests the information from the user and updates its database.

A translation application tool translates a web page from its native language into a default language or a language of the user's choice. The tool transmits the context web page (or a link to the context web page) to a translation server, which produces a results web page that is sent to a client tool window for display. For one translation server, the tool transmits a URL in which is embedded as an argument the URL of the web page to be translated.

A say-it application tool speaks the current context web page. This tool operates like the translation tool in obtaining the speech data stream, and it illustrates the point that an application tool need not produce a web page as output.

A login helper application tool maintains a database of login names and passwords for the user. When the user is at a web site that requests or requires a user name and password, the user can click on the login helper icon on the bar. If the current context is not a site that the login helper tool recognizes as one for which the tool database contains a name and password, the tool opens a client tool window for the user to enter the name and password the user has selected for the current context. This information is maintained on a database by the login helper tool server. If the current context is a site that the login helper tool does recognize as one for which the database contains a name and password, the tool autofills the site's name and password form, if the form is one that can be filled, or the tool provides the name and password so that the user can cut and paste into the site's input page. The user can protect use of this tool with a password.

An e-mail monitor application tool assists the user in monitoring the user's various e-mail sites. The user adds sites to an e-mail list by navigating to the site, which becomes the current context, opening the tool through the monitor tool icon on the bar, and selecting an add-to-list option. The tool requests the user's e-mail address and password and stores the information in a tool database. The tool visits each site on the monitoring list by HTTP request at a user-selected time interval, using the information in the database to respond to the site's request for name and password. The tool then calculates a signature for the resulting web page and compares it to the previously calculated signature. If the signatures differ, the user is notified by animation of the tool icon on the bar. The signature can be calculated using any convenient hashing or message digest algorithm, such as MD5. The user can protect use of this tool with a password.

A web rings application tool connects affinity groups of users to others within their group. A group member can add a site to a collection by browsing to the site to make the site the context, opening the tool, and selecting an option to add the current site to the collection. The members of the group can view the group's collection or collections of links on a client tool window and use those links to browse to the sites themselves. When a user opens such a link, the client causes a new web browser window to be opened to display the site. This is done so that the site becomes the current context and the user's other active tools can respond to the site.

A comparative shopping application tool makes price, feature and benefit comparisons. When the user opens the shopping tool icon on the bar, the tool searches its database for pricing, feature, and promotional information and links for products of the kind shown in the current context web page. The tool presents this information in tabular form in a client browser window, and the user can sort the information, by price or manufacturer for example, and browse from the information to vendors' or manufacturers' sites.

A retail registry application tool enables users to register for gifts at retail sites. To register for a gift, a member simply

clicks on the registry icon on the bar when the context is a web page corresponding to or displaying the desired gift. The registering user can optionally open the tool to add further information, such as color, size, or quantity, which is maintained in a tool database. To view the registry, a user opens the tool and enters a screen name or other information to identify the registered member. The tool displays a page of links and further information. The user can use the links to browse to vendors' or manufacturers' sites, which will be displayed in a web browser window, which will become the active web browser window so that the target site becomes the current context and other active tools can respond to the site. The purchasing user can add to the database information, for example by indicating that an item on the registry will be purchased by the user, or that the user will contribute to the purchase of the item.

Administrative Functions

The System includes a number of pages and subsystems to support administrative functions. The administrator page is a password-protected web page that provides access to administrative functions and information. The administrator page is accessed by URL address. It has links to the administrative status page. The administrative status page includes links to various status reports including reports of use statistics. System subsystems include a System Monitor subsystem that monitors the System for integrity and updates an administrator monitor page on an automatic and timed basis. In addition, if it detects a problem, it notifies the System administrator by e-mail and by audible and visual alert at the administrator monitor page. The administrator monitor page is protected by password and user ID. It shows when it was last updated (day/time) and the results of the most recent test of System integrity.

The invention can be implemented in digital electronic circuitry, or in computer hardware, firmware, software, or in combinations of them. Apparatus of the invention can be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor. Method steps of the invention can be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output. The invention can be implemented advantageously in one or more computer programs that are executable on a programmable computer system including at least one programmable processor coupled to receive data and instructions from, and to transmit data and instructions to, a data storage system, at least one input device, and at least one output device. Each computer program can be implemented in a high-level procedural or object-oriented programming language, or in assembly or machine language if desired; and in any case, the language can be a compiled or interpreted language. Suitable processors include, by way of example, both general and special purpose microprocessors. Generally, a processor will receive instructions and data from a read-only memory and/or a random access memory. Storage devices suitable for tangibly embodying computer program instructions and data include all forms of nonvolatile memory, including by way of example semiconductor memory devices, such as EPROM, EEPROM, and flash memory devices; magnetic disks such as internal hard disks and removable disks; magneto-optical disks; and CD-ROM disks. Any of the foregoing can be supplemented by, or incorporated in, ASICs (application-specific integrated circuits).

To provide for interaction with a user, the invention can be implemented on a computer system having a display device such as a monitor or LCD screen for displaying information to the user and a keyboard and a pointing device such as a mouse or a trackball by which the user can provide input to the computer system. The computer system can be programmed with an operating system such as Microsoft Windows 95 that supports graphical user interfaces through which computer programs interact with users.

Tables

This specification includes the following tables, which show example interactions, pages, and messages that can arise during use of the System: Table A, Illustrative User-System Interactions (for Basic Service); Table B, Illustrative User-System Interactions (for Discussion Tool); Table C, Illustrative System Interactions (Administrative); Table D, Description of Illustrative System Web Pages; and Table E, Description of Illustrative Service E-mail Messages.

Conclusion

The invention has been described in terms of particular embodiments. Other embodiments are within the scope of the following claims. For example, the steps of the invention can be performed in a different order and still achieve desirable results. In addition, a server does not necessarily correspond to a computer. A server may be implemented on a computer that runs multiple servers, and a single server may be implemented on multiple computers in one or more locations. The bar can be implemented with free-standing icons, which can be placed on or relative to the active web browser window. The bar can be moved off of the active web browser window unless that window fills the display screen.

TABLE A

Illustrative User-System Interactions (Basic Service)

INTERACTION #1
Potential Member Downloads, Installs Service

OVERVIEW

Goal in Context	To download and install the Service and submit profile.
Success End Condition	Potential member receives e-mail verification of profile.
Trigger	New potential member goes to Service web site and clicks [DOWNLOAD/INSTALL].

DESCRIPTION OF MAIN FLOW

Step	Action
1	Potential member arrives at Service web site; Service displays download instructions; user selects [DOWNLOAD/INSTALL].
2	Service identifies user's web browser.
3	Service determines that the web browser is supported, e.g., Internet Explorer 4.01 ("IE").
4	Service loads software and member views Standard Microsoft Signature system Security Warning screen with question "Do you want to install and register? [YES], [NO], [MORE INFO]"
5	Member clicks [YES].
6	Service installs client software, places Service start icon in the Windows links bar and Windows quicklaunch bar and places start command in the IE context menu; client displays the bar and the Modified Profile page.
7	Member views Modified Profile page.
8	Member fills in at least the mandatory fields and selects [Submit Registration].

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

9	Service verifies that at least the mandatory fields are filled in with valid data; generates e-mail verification to the member's e-mail address.
10	Service sends e-mail verification to member.

DESCRIPTION OF BRANCHING ACTION

Step	Action
3	Service detects that member's web browser is not supported.
3a	Member views Unavailable Browser message page.
4	Member clicks [NO].
4a	Member is retumed to Step 1, above.
4	Member clicks [MORE INFO].
4b	Member views Microsoft Standard Internet Certification message - only option at this screen is to close and go back to Step 1.
8	Member closes out of Profile page without submitting registration.
8a	Member views blank bar. See Interaction #3.
9	Service determines that the mandatory fields were not filled in or that the data was invalid.
9a	Member views Mandatory Fields or Format message page.
9b	Member is retumed to Step 7, above.
10	Service receives bounced back message-determines that the e-mail address is not valid.
10a	Member is not registered with Service.

INTERACTION #2
Potential Member Receives B-mail Verification of Registration and Completes Registration Process

OVERVIEW

Goal in Context	To complete registration and be recognized by the Service.
Preconditions	Member has submitted registration to the Service and has received verification e-mail.
Success End Condition	Member receives user ID (cookie) and views bar.
Trigger	Member clicks on URL link to Thanks for Registering web page that is displayed in member's verification e-mail.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on URL link to Thanks for Registering web page that is displayed in member's Verification e-mail . . . views Verification e-mail.
2	Member clicks on the URL link to the Service Thanks for Registering web page.
3	Member arrives at the Thanks for Registering web page.
4	Service determines that the member has a unique e-mail address in the database and assigns a user ID.
5	Service downloads user ID to member's web browser in the form of a cookie.
6	Service recognizes member by user ID and displays the bar.

DESCRIPTION OF BRANCHING ACTIONS

Step	Action
2	Member does not click on the link.
2a	Member is not recognized by the Service. The member's bar stays blank.
4	Member has cookies turned off.
4a	Member views Tum Cookies On message page.
4	Service determines that the e-mail address is not unique in the database (for example, member is already registered but is registering again from another computer).

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

4a	Service matches member with member's existing user ID and uploads member's user ID to member's web browser in the form of a cookie.

INTERACTION #3
Potential Member Views Blank Bar

OVERVIEW

Goal in Context	To view blank bar.
Preconditions	Potential member has downloaded and installed the Service but has not visited the Thanks for Registering page (or member's browser does not accept cookies).
Success End Condition	Potential member views blank bar.
Trigger	Potential member logs into web browser or closes profile form after Download/Installation.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Potential member logs into web browser or closes profile form after Download/Installation.
2	Potential member views blank bar.

DESCRIPTION OF BRANCHING ACTIONS

2	Potential member clicks [here] link to register.
2a	Potential member views Modified Profile page. See Interaction #6.
2	Potential member selects Help from the options menu.
2a	Potential member views Online Help page. See Interaction #7.
2	Potential member selects Send Feedback from the options menu.
2a	Potential member views default e-mail compose window. See Interaction #8.
2	Potential member selects Uninstall from the options menu.
2a	Potential member views Uninstall page. See Interaction #11.

INTERACTION #4
Member Views Bar

OVERVIEW

Goal in Context	To view an up-to-date bar for active, open web browser window.
Preconditions	Client is running.
Success End Condition	Member views bar, which is updated for every URL member browses to.
Failed End Condition	Bar displays an error message.
Trigger	Member launches web browser.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member launches web browser which launches client; Service recognizes that the member is a registered member by user ID (cookie).
2	Service checks version of the Service to determine that it is current.
3	Service displays bar. Content of the bar depends on the specific tools being delivered by the Service.

DESCRIPTION OF BRANCHING ACTIONS

2	Service determines that the member's version of the Service is out of date.
2a	Member views Upgrade Service message page. If member clicks [Yes], member views the Service Download/Install web page. If member clicks [No], the message page goes away and member continues.
2	Service determines that previous e-mails generated and sent by the Service have been bounced back as undeliverable.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

2a	Member views Bounced E-mail message page. If member clicks [Leave it alone], the page closes and member continues. If member clicks [Update], member is redirected to the Profile page.
3	Member browses to another URL by changing the URL of member's current web browser window.
3a	Service or application tool updates icons on bar with information or status that is current to the URL of the web browser window.
3	Member browses to another URL by opening multiple web browser windows.
3a	Bar is visible for current open web browser window only.

INTERACTION #5
Member Views Options Menu

OVERVIEW

Goal in Context	To view options menu.
Preconditions	Member is viewing the bar.
Success End Condition	Member views options menu.
Trigger	Member clicks on the Service logo on the bar.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the Service logo on the bar.
2	Service displays the options menu.

INTERACTION #6
Member Views Profile and Edits Profile Info

OVERVIEW

Goal in Context	To access and edit the profile info.
Preconditions	Member is viewing the options menu.
Success End Condition	Changes to profile are successfully submitted to the Service and member views them on the Profile page.
Failed End Condition	Changes to profile are not submitted to the Service; member does not view changes made to the Profile page.
Trigger	Member clicks on the Service logo on the bar and selects Profile from the options menu.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the Service logo on the bar and selects Profile from the options menu; Service displays Standard Profile page.
2	Member enters new data into the fields on the Profile page.
3	Member clicks on the [Submit Changes] button.
4	Service checks to determine that all mandatory fields are filled in and data is in correct format.
5	Service determines mandatory fields are filled in, data is in correct format, and changes edited fields in the database.

DESCRIPTION OF BRANCHING ACTIONS

5	Service determines mandatory fields are not filled.
5a	Service returns Mandatory Fields message page.
5b	Member returns to Step 2.
5	Service determines data is not in correct format.
5a	Service returns Format message page.
5b	Member returns to Step 2.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

INTERACTION #7
Member Requests Help

OVERVIEW

Goal in Context	To request online help.
Preconditions	Member is viewing the options menu.
Success End Condition	Member views online help pages.
Trigger	Member clicks on the Service logo on the bar and selects Help from the options menu.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on Help on the options menu.
2	Service displays Online Help web page in a new client browser window.

INTERACTION #8
Member Sends Feedback

OVERVIEW

Goal in Context	To send feedback to Service administrator.
Preconditions	Member is viewing the bar.
Success End Condition	Member sends feedback to the Service administrator.
Trigger	Member clicks on the Service logo on the bar and selects Send Feedback from the options menu.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on Send Feedback on the options menu.
2	Service displays Member's default e-mail compose window. To: feedback@the_system.com
3	Member enters subject and message and sends e-mail.

INTERACTION #9
Member Disables Service

OVERVIEW

Goal in Context	To stop viewing the bar.
Preconditions	Member is viewing the options menu.
Success End Condition	Member disables the Service and the bar is not visible.
Trigger	Member clicks on the Service logo on the bar and selects Close from the options menu or on the close box on the bar.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the Service logo on the bar and selects Close from the options menu or on the close box on the bar.
	Service closes bar.
	Note: Bar stays closed until member goes to the Service link in the Windows links bar or Windows quicklaunch bar or context menu to reenable it.

INTERACTION #10
Member Re-Enables Service

OVERVIEW

Goal in Context	To re-enable the Service after it has been closed; to see the bar.
Preconditions	Service has been closed. Member is within member's web browser.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

Success End Condition	Member re-enables member's Service and sees the bar.
Trigger	Member clicks on the Service logo on a Windows links bar or quicklaunch bar, or in a context menu.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the Service start icon.
2	Client launches and Service displays the bar.

EXTENSIONS OF BRANCHING ACTIONS

2	Member is in another application and has web browser open in the background.
2a	Client makes the web browser the active application and displays the bar.
2	Member is in another application and does not have web browser open in the background.
2a	Client opens member's default web browser, navigates member to the Service web site and displays the bar.

INTERACTION #11
Member Uninstalls Service

OVERVIEW

Goal in Context	To uninstall the Service from computer.
Preconditions	Member has installed the Service. Member is viewing the options menu.
Success End Condition	Member successfully uninstalls Service.
Trigger	Member selects Uninstall from the options menu.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member selects [Uninstall] from the options menu.
2	Service displays Uninstall message page.
3	Member clicks [Uninstall] on Uninstall page.
4	Service runs Uninstall program to remove the application and to notify the Service that the member uninstalled. (Uninstalled users are tracked in the Service database.)
5	Member views Uninstall Comments message page.
6	Member enters comment and e-mail address and clicks [OK]

DESCRIPTION OF BRANCHING ACTIONS

2	Member clicks [Close]
2a	Service is closed.

INTERACTION #12
Service Receives Mail That Is Bounced Back

OVERVIEW

Goal in Context	To mark member's record in the database when Service-generated e-mail has bounced.
Preconditions	E-mail has been sent to the member and has been bounced back as undeliverable.
Success End Condition	Next time member logs onto the Service, member views "Bounced Back E-mail" message.
Trigger	Service-generated e-mail has been bounced back as undeliverable.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

DESCRIPTION OF MAIN FLOW

Step	Action
1	Service-generated e-mail has been bounced back as undeliverable.
2	Service marks member's record in the database as having had mail bounced back.

INTERACTION #13
System Monitor Checks That Service Is Operational

OVERVIEW

Goal in Context	To issue query against the Service web server and, by receiving returned value, determine that the Service is operational.
Success End Condition	System Monitor receives expected returned value.
Failed End Condition	System Monitor does not receive expected returned value.
Trigger	System Monitor is activated 1) as a regular, timed function controlled at the configuration file or 2) manually at the Administration Monitor page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	System Monitor is activated 1) as a regular, timed function controlled at the Configuration File or 2) manually at the Administration Monitor page.
2	System Monitor issues query to web server.
3	System Monitor receives correct returned value.
4	System Monitor updates Administration Monitor page with time/date and results of System Monitor check.

DESCRIPTION OF BRANCHING ACTIONS

3	System Monitor receives incorrect returned value or does not receive response.
3a	System Monitor updates Administration Monitor page with time/date of System Monitor check and results and activates animation and audible alarm at the Administration Monitor page.
3b	System Monitor generates and sends "Problem with Service" e-mail to addresses that are in the configuration file.

INTERACTION #14
Administrator Logs in to Administration Page

OVERVIEW

Goal in Context	To gain access to administrative functions.
Preconditions	Administrator must know the Login page's password.
Success End Condition	Administrator views Administration page.
Failed End Condition	Administrator views "Login Failed" message.
Trigger	Administrator navigates to Administrator Login page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Administrator navigates to Administrator Login page.
2	Service displays Administrator Login page.
3	Administrator enters password.
4	Service checks to determine if the password is correct.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

5 Service determines password is correct.
6 Service displays Administration page.

DESCRIPTION OF BRANCHING ACTIONS

5 Service determines password is incorrect.
5b Administrator views "Login Failed" message.

INTERACTION #15
Administrator Views Administration Monitor Page

OVERVIEW

Goal in Context	To view Administration Monitor page.
Preconditions	Administrator must be viewing the Administration page.
Success End Condition	Administrator views Administration Monitor page.
Trigger	Administrator clicks on the link to the Administration Monitor page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Administrator clicks on the link to the Administration Monitor page.
2	Service displays Administration Monitor page.

INTERACTION #16
Administrator Views Administration Status Page

OVERVIEW

Goal in Context	To view Administration Status page.
Preconditions	Administrator must be viewing the Administration page.
Success End Condition	Administrator views Administration Status page.
Trigger	Administrator clicks on the link to the Administration Status page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Administrator clicks on the link to the Administration Status page.
2	Administrator views Administration Status page.

INTERACTION #17
Administrator Manually Activates System Monitor

OVERVIEW

Goal in Context	To activate the System Monitor manually.
Preconditions	Administrator must be viewing Administration Monitor page.
Success End Condition	Administrator views refreshed Administration Monitor page.
Trigger	Administrator clicks on the [Run Administration Monitor] button on the Administration Monitor page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Administrator clicks on the [Run Administration Monitor] button on the Administration Monitor page. See Interaction #14.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

INTERACTION #18
Administrator Views/Hears Notification From Administration Monitor That There Is a Problem With the Service

OVERVIEW

Goal in Context	To view and hear notification of System Monitor alert.
Preconditions	Administrator has logged into Administration Monitor page.
Success End Condition	Administrator views and hears notification of System Monitor alert at the Administration Monitor page.
Trigger	System Monitor detects a problem with the Service and updates Administration Monitor page. See Interaction #14.

DESCRIPTION OF MAIN FLOW

Step	Action
1	System Monitor detects a problem with the Service and updates Administration Monitor page.
2	Administration Monitor page flashes madly and plays a warning sound continuously.

INTERACTION #19
Administrator Edits Configuration File

OVERVIEW

Goal in Context	To edit Configuration File.
Preconditions	Administrator views Configuration File.
Success End Condition	Administrator views edits in Configuration File.
Trigger	Administrator opens Configuration File and edits the text.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Administrator opens Configuration File and edits the text.

INTERACTION #20
Member Resizes the Bar

OVERVIEW

Goal in Context	To resize the bar.
Preconditions	Member is viewing the bar.
Success End Condition	Member views bar at its new size.
Trigger	Member resizes window.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member resizes bar window.
2	System displays resized bar.

INTERACTION #21
Member Views Privacy Page

OVERVIEW

Goal in Context	To view Privacy page.
Preconditions	Member is viewing the Help page.
Success End Condition	Member views Privacy page.
Trigger	Member clicks on the Privacy Policy link on the Help page.

TABLE A-continued

Illustrative User-System Interactions (Basic Service)

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on Privacy Policy on the Help page.
2	Service displays Privacy page.

TABLE B

Illustrative User-System Interactions (Discussion Tool)

INTERACTION #30
Member Opens Discussion Tool

OVERVIEW

Goal in Context	To open the Discussion Tool application
Preconditions	Member has installed user platform, registered with the System, and installed Discussion Tool.
Success End Condition	Member opens Discussion Tool and views Billboard page.
Trigger	Member clicks on the Discussion Tool icon in the bar.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the Discussion Tool icon in the bar.
2	Member views Billboard page.

INTERACTION #31
Member Controls Change of Displayed Billboard Comments

OVERVIEW

Goal in Context	To change manually which Billboard comment is displayed by scrolling forward or backward in the list.
Preconditions	Member is on the Billboard page.
Success End Condition	Member manually is able to change which Billboard comment is displayed.
Trigger	Member clicks on the [+] button on the Billboard page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the [+] button on the Billboard page.
2	Displayed Billboard comment advances by one.
3	Member views new comment and counter number advanced.

DESCRIPTION OF BRANCHING ACTIONS

1	Member clicks on the [−] button on the Billboard page.
1a	Displayed Billboard comment reverts to previous comment.
1b	Member views previous comment and counter number.

INTERACTION #32
Member Adds Comment to Billboard

OVERVIEW

Goal in Context	To add comments to Billboard list.
Preconditions	Member is on Billboard page.
Success End Condition	Member add new comment to Billboard list and sees it displayed.
Trigger	Member clicks into Billboard comment field.

TABLE B-continued

Illustrative User-System Interactions (Discussion Tool)

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks into Billboard comment field.
2	Add Billboard Comment page is displayed.
3	Member types in comment.
4	Member clicks on [OK] button.
5	Add Billboard Comment page is closed and Member views member's comment as current comment on Billboard screen.

DESCRIPTION OF BRANCHING ACTIONS

4	Member clicks on [Cancel] button.
4a	Add Billboard Comment page is closed and member goes back to member's previous view of Billboard page.

INTERACTION #33
Member Closes Billboard Page

OVERVIEW

Goal in Context	To close Billboard page.
Preconditions	Member is on Billboard page.
Success End Condition	Member closes Billboard page.
Trigger	Member clicks on the [Close] button on Billboard screen.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the [Close] button on Billboard screen.
2	Billboard screen closes.

INTERACTION #34
Member Opens Topic Page

OVERVIEW

Goal in Context	To open Topic page.
Preconditions	Member is on Billboard page
Success End Condition	Member views Topic page.
Trigger	Member clicks on [Discussion Topics] button.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on [Discussion Topics] button.
2	Member views Topic page in Splash Screen mode.

INTERACTION #35
Member Adds New Topic to Topic List

OVERVIEW

Goal in Context	To add new topic to Topic list.
Preconditions	Member is on Topics page.
Success End Condition	Member adds new topic and is prompted to add first comment to new discussion.
Trigger	Member clicks into New Topic field.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks into New Topic field.
2	Member types in title of new topic.
3	Member clicks on the [OK] button.
4	Member views member's newly created topic as the selected topic in the Topic list.

TABLE B-continued

Illustrative User-System Interactions (Discussion Tool)

5 Topic page view changes from Splash Screen mode to Add mode.

DESCRIPTION OF BRANCHING ACTIONS

3 Member does not click on the [OK] button.
3a His new topic title does not become a topic in the Topic list.

INTERACTION #36
Member Adds First Comment

OVERVIEW

Goal in Context	To add first comment in newly created discussion topic.
Preconditions	Member is viewing blank Add mode of Topic page; just entered new topic.
Success End Condition	Member views member's new comment as first comment in newly created discussion topic.
Trigger	Member enters comment subject in Subject field.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member enters comment subject in Subject field.
2	Member enters e-mail addresses into copy-to field if member wants to invite another member.
3	[Personal Message] button becomes activated.
4	Member enters comment into Post Message field.
5	Member clicks [OK].

DESCRIPTION OF BRANCHING ACTIONS

2a Member does not enter e-mail address into copy-to field.
2b [Personal Message] button remains greyed out (inactive).
5a Member has not entered comment.
5b Member views Mandatory Fields message page.
5a Member clicks on [Personal Message] button.
5b See Interaction #37

INTERACTION #37
Member Invites Another Member or Potential Member

OVERVIEW

Goal in Context	To send e-mail invitation to member or potential member, inviting them to view a particular discussion.
Preconditions	Member is on Add mode of Topic page, has entered e-mail address or addresses into the copy-to field.
Success End Condition	Member sends e-mail invitation to another member or potential member.
Trigger	Member clicks on the [Personal Message] button on the Add mode of Topic page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the [Personal Message] button on the Add mode of Topic page.
2	Member views Personal Message view of Add page.
3	Member types a personal message into Personal Message field.
4	Member clicks [OK] button.
5	System compares e-mail address in copy-to field to e-mail addresses of registered members in database and determines that e-mail address matches.
6	System generates "Registered Member Invitation" e-mail and sends it to members.

TABLE B-continued

Illustrative User-System Interactions (Discussion Tool)

DESCRIPTION OF BRANCHING ACTIONS

3 Member does not enter a personal message into the Personal Message field.
3a System generates e-mail invitation without a personal message.
4 Member clicks [radio button] Include client software.
4a System includes client software in the e-mail invitation.
4 Member clicks [Cancel]
4b Member views Add mode in Posted Message view.
5 System compares e-mail address in copy-to field to e-mail addresses of registered members in database and determines that e-mail address does not match that of any registered member.
5a System generates "Non Member Invitation" e-mail and sends it to potential members.

INTERACTION #38
Member Views Topic Page in Read Mode

OVERVIEW

Goal in Context	To view the Topic page in Read mode.
Preconditions	Member is either on Topic page in Splash Screen mode or on Topic page in Add mode.
Success End Condition	Member views Topic page in Read mode.
Trigger	Member clicks on [Read] button on Add mode page or on a topic in Topic list on Splash Screen mode page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on [Read] button on Add mode page or on a topic in Topic list on Splash Screen mode page.
2	Member views Read mode page for the selected topic.

INTERACTION #39
Member Closes Topic Page

OVERVIEW

Goal in Context	To close Topic page.
Preconditions	Member is on Topic page.
Success End Condition	Member closes Topic page and views Billboard page.
Trigger	Member clicks on [Close] button.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on [Close] button on Topic page.
2	Topic page closes.
3	Member views Billboard page.

INTERACTION #40
Member Prevents a Discussion From Expiring

OVERVIEW

Goal in Context	To vote that a discussion is of value to prevent expiration of discussion.
Preconditions	Member is on Discussion Tool home page; there are discussions on top pane of the page.
Trigger	Member clicks on click [here] link to cast vote.

TABLE B-continued

Illustrative User-System Interactions (Discussion Tool)

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member views message "If you like this discussion, click [here]. (It will stay longer)." at the bottom of the comments on the page.
2	Member clicks on the click [here] link.
3	Service recomputes the discussion's time until expiration.
3	Member views new time until expiration.

DESCRIPTION OF BRANCHING ACTIONS

2	Time until expiration is maximum value (e.g., six months).
2a	Member views Maximum Time Until Expiration message page.
2b	Member is returned to Step 1.

INTERACTION #41
Member Receives/Views Invitation

OVERVIEW

Goal in Context	To provide for registered members and/or (unregistered) potential members to be invited to a discussion.
Preconditions	Intended recipient of the invitation must have a valid e-mail address; member's e-mail address must be entered into the copy-to field.
Success End Condition	Intended recipient receives and views e-mail invitation to a discussion.
Trigger	Registered member or potential member opens an invitation e-mail message.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Recipient receives and views e-mail invitation.
2	Registered member clicks on the URL link to the discussion. - or - Potential member clicks on URL link to the Download/Install web page.

DESCRIPTION OF BRANCHING ACTIONS

2	Potential member clicks on the URL link to the discussion.
2a	Potential member views You Are Not Registered page.

INTERACTION #42
Member Navigates to Another URL Through a Link in, a Comment

OVERVIEW

Goal in Context	To navigate to a different web page through a link in a comment on Topic page.
Preconditions	Member is viewing Topic page in Read mode; views comment with a URL link in it.
Success End Condition	Member navigates to another web page.
Trigger	Member clicks on the URL link in a comment.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the URL link in a comment.
2	Member views new web page in a client browser window. See Interaction #44 (Member navigates to new URL with Discussion Tool open).

TABLE B-continued

Illustrative User-System Interactions (Discussion Tool)

INTERACTION #43
Member Navigates to Discussion Through a URL Link

OVERVIEW

Goal in Context	To navigate to a discussion by clicking on a URL.
Preconditions	Member is viewing an invitation.
Success End Condition	Member clicks on link to a discussion and views the Topic page in Read mode with the discussion to which member was invited as the selected topic.
Trigger	Member clicks on the link to a discussion.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member clicks on the link to a discussion.
2	Member navigates to the discussion's URL. Note: Discussion Tool includes an "on open" property for the Topic page that opens another window with the corresponding web page from which it was created.
3	Member views Topic page Read mode with the discussions'topic selected.

DESCRIPTION OF BRANCHING ACTIONS

1	Member clicks on URL to a discussion that has expired.
1a	Member views Discussion Has Expired message page.

INTERACTION #44
Member Navigates to a New URL with Discussion Tool Open

OVERVIEW

Goal in Context	To navigate to another URL while Discussion Tool is open at current web site or to click between multiple open web browser windows.
Preconditions	Member is viewing Topics page in Read or Add mode.
Success End Condition	Member navigates to another URL and views new Topic page for that web site.
Trigger	Member enters URL into address field of web browser or clicks on link to another web page.

DESCRIPTION OF MAIN FLOW

Step	Action
1	Member's Topic page closes.
2	Member navigates to new web page.
3	Topic page is opened in Read mode with default topic selected.

DESCRIPTION OF BRANCHING ACTIONS

3	Member was in Splash Screen mode on previous page
3a	Topic page is opened in Splash Screen mode.

TABLE C

Illustrative System Interactions (Administrative)
INTERACTION #50
System Records Service Activity in Log

OVERVIEW

Goal in Context	To record various Service activities in System Log.

TABLE C-continued

Illustrative System Interactions (Administrative)
INTERACTION #50
System Records Service Activity in Log

DESCRIPTION OF MAIN FLOW

Event	Logged Information
Install	who, when, upgrade
Uninstall	who, when
Close	who, when
Login	who, when
Discussion viewing	who, when
Comment viewing	who, when
Comment creation	who, when, URL, which discussion, simple URL
Discussion creation	who, when, URL
Invitation	from, to, about, when, follow-ups
Registration	who, when, wherefrom, re-register
Web site viewing	who, when, URL, simple URL
Help viewing	who, when, what part

TABLE D

Description of System Web Pages

Page Title and Description

(Buttons and links are denoted by text enclosed in "[ ]".)
(Comments enclosed in "( )" are not displayed.)
System Home page

[Explanation of Service]
[Download and Install]
[Member Services]
[Help]
[Feedback]
Download/Install page

Service Requirements
Download and installation instructions
[Download/Install]
Service logo
Upgrade Service page

"You are running an older version of the Service. An upgraded version is available offering the following new features:"
List of features.
"If you would like to upgrade now, click [here]"
(link takes user to Install/Download page)
"To continue with the Service version you are currently using, click [here]" (link takes user back to user's browser home page)
Thanks for Registering page

(Accessed through link from verification e-mail.
When user arrives, user is assigned a user ID.
User ID is uploaded in a cookie.)
"Your registration is complete. Welcome to the Service!
If you registered because a friend told you about a discussion that you might be interested
in, go back to your e-mail and click on the link to the discussion.
If you would like to view sites where there is current discussion activity, follow one of the links below."
List of "hot sites"places where there are active discussions.
[Feedback]
Options menu

[Help] (Privacy Policy)
[Profile]
[Close]
[Uninstall]
[Feedback]
[Credit]
Standard Profile page

(This page is accessed from the Profile link from the options menu)
Two fields for name

TABLE D-continued

Description of System Web Pages

Field for Screen name
Field for User ID (noneditable field) (will be filled in by the Service)
Field for e-mail address
"Do you wish to receive e-mail notification and invitations? [yes] [no]"
(Optional information can include:
drop down list for gender
drop down list for age
drop down list for occupation)
[OK]
logo
Modified Profile page

Modified Profile page is the first screen displayed after installation is complete. "Thank you for downloading and installing the Service. Your installation is complete.
To complete your registration and activate your Service, please fill in the following information and click on the Submit Registration button. You will receive a confirmation via e-mail within a few minutes."
All fields listed on Standard Profile page
[Submit Registration] button
logo
Uninstall page

Accessed from the Uninstall link from the options menu
"Thanks for trying the Service . . . Uninstalling the Service will remove it from your computer. If you would rather leave it installed and just make it go away temporarily, click here to disable (this is a link) instead of uninstall.
If you disable the Service, you can make it visible again by simply clicking on the link in your links bar or your quick launch bar. If you want to continue and remove the Service, click here to uninstall (this is a link)
and then restart your web browser."
logo.
Uninstall Comments page

"Restart your browser to complete the uninstall.
We would appreciate your comments on why you've chosen to remove the Service, so that we can improve it to better meet your needs.
[radio button] Not Useful
[radio button] Annoying
[radio button] Slow
[radio button] Unreliable
[radio button] Crashes"
[radio button] Comment field
E-mail field
[OK]
logo
You Are Not Registered page

"You are not a registered member of the Service.
You must download and install the
Service and submit your registration. To download/install, click[here]." (link to Download/install page).
Discussion Has Expired page

"You have requested to view a discussion that has expired.
It is no longer available."
Invitation page

field for topic of the discussion (this will be filled in with the topic of the selected discussion or, if the invitation is being made from the bar, with the General Discussion topic.
field for e-mail addresses of people to invite (mandatory)
field for a custom message (not mandatory)
[OK] button
[Cancel] button
Mandatory fields indicated in red.
New Discussion page

Field for topic of the discussion
Field for a list of e-mail addresses to invite (optional)
[OK]
[Cancel]

TABLE D-continued

Description of System Web Pages
Unavailable Browser message page
logo "Your current browser is (name of browser). The (name of browser) version of the Service is not available yet. Please enter your e-mail address and you will be notified as soon as it is available." Mandatory Fields message page
logo "Please fill in all mandatory fields. Mandatory fields are indicated." Format message page
logo "E-mail address or screen name is not in the correct format." Turn Cookies On message page
logo "In order to use the Service, you must have cookies turned on. To turn on cookies, (browser-specific instructions)." Maximum Time Until Expiration message page
"Maximum time until expiration is 6 months." Online Help page
Search and navigation for Service help information. Bounced E-mail message page:
logo "The last e-mail we sent you was undeliverable. Do you want to update your e-mail address so we can send you e-mail in the future? [Leave it alone] (a URL link) - or - [Update] (a URL link) your e-mail address for our records so we can start sending you e-mail again. (If your e-mail address has not changed, select this option anyway and let us know it's the same.)" Upgrade message:
logo "Good news! A new version of the Service is available. Upgrading now only takes a minute and does not require you to reboot. Would you like to upgrade now?" [Yes] [Not right now]" Privacy page
logo (privacy policy) Comment page
Comment subject field Comment text box [OK] Administration Status page
logo Includes links to various status reports including: Web Trends Statistics Number of Members Registered Number of Members Logged In Number of Members vs. Time Number of Comments vs. Time Number of Discussions vs. Time Number of Sites vs. Time Ordered list of Top Sites By Activity/Visits By Discussion/Comments Ordered List of Top Members Ordered list of Top Discussion Ordered List of Top Subscriptions Mean Lifetime of Discussions Votes with Most Responses Discussion Expiration Statistics

TABLE D-continued

Description of System Web Pages
Administration Monitor page
logo Last time Administration Monitor checked Service Results (Service is OK) or (Service Alert) [Run Administration Monitor] button to execute System check manually
Administrator Login page
logo "Enter your User name and password" field for User name field for Password The Administration page
The Administration page is accessed through URL address. It is protected by password and user ID. Page can blink or animate in some way to graphically call attention if System Monitor reports problem with the Service Page has audible notification to call attention if System Monitor reports problem with the Service. Link to Administration Monitor page. Link to Status page.

TABLE E

Description of Illustrative Service E-mail Messages

Message No.	Title Description
1	Send Feedback e-mail message This is accessed from the Send Feedback link off the options menu. To: Feedback@the_service.com.
2	Verification e-mail message To: [e-mail address] From: Registration@the_service.com Subject: Thanks for Registering with the Service! "Thank you for registering with the Service. Click on the link below to receive your User ID and to activate your Service. Note: you must have cookies turned on in order to activate the Service. [URL link to Thanks for Registering page]
3	If you ever want to turn off the Service, see the Disable command on the options menu (you can see the Options Menu by clicking on the Service logo on your Bar." Registered Member Invitation e-mail message From: [e-mail address of sender] To: [e-mail address of recipient] Subject: Invitation to a Discussion [Screen name] ([e-mail address]) invites you to a discussion about: [web site]. [Screen name] says: [sender's comments] To go to the discussion, click this link: [URL to discussion] Enjoy! P.S. If you need to reinstall the Service, go to: [URL to the download page]
4	New Member Invitation e-mail message From: [e-mail address of sender] To: [e-mail address of recipient] Subject: Invitation to a Discussion [Screen name] ([e-mail address]) invites you to a discussion about: [web site] [Screen name] says: [sender's comments] To see the discussion, you need to register with the Service. It's easy, quick, and free! To register, go to: [URL to the download page] Once you're done with registration, go to [URL to discussion] to see the discussion. Enjoy!

TABLE E-continued

Description of Illustrative Service E-mail Messages

Message No.	Title Description
5	Problem With Service e-mail message To: [e-mail address] From: SystemMonitor@the_service.com Subject: Service Alert! "The System Monitor has detected a problem with the Service." [URL link to Administrator Login page]

What is claimed is:

1. A method for providing information to a user browsing the web, comprising:

presenting to the user one or more application tools that the user may enable and disable;

transmitting a context defined by the user's browsing activity to a user-selected and enabled application tool;

generating a web page parallel to the actual web page being visited by the user, wherein generating the web page includes running the application tool to generate a reaction to the context for the user; and

displaying the parallel web page.

2. The method of claim **1**, wherein the parallel web page is generated by a server operating independently of the web site providing the actual web page.

3. The method of claim **1**, wherein the parallel web page is generated by a discussion tool.

4. The method of claim **1**, wherein the parallel web page is generated by a contextual sales tool.

5. The method of claim **1**, wherein the parallel web page is generated by a web ring tool.

6. The method of claim **1**, wherein the parallel web page provides an interface for the user to interact with a computer program tool operating independently of the actual web page or the web browser.

7. The method of claim **6**, wherein the tool is a comparative shopping tool.

8. The method of claim **1**, further comprising:

presenting to the user an interface for a computer program tool;

transmitting context information derived from the user's browsing activity with the web browser to the tool; and

using the context information in the tool to generate the parallel web page.

9. The method of claim **1**, wherein the parallel web page is generated to notify the user that a computer program tool has information relevant to the actual web page.

10. The method of claim **9**, wherein the computer program tool is operable to read the requested web page.

11. A method of providing information to a user of a user computer, comprising:

providing a first web browser to run on the user computer, the first web browser being a conventional web browser, the user interacting with the first web browser through conventional web browsing user interface actions; and

providing a client program providing a client user interface separate from that of the first web browser, the client program receiving first information from the first web browser about activity occurring on the first web browser, the client program providing outputs to the user in response to the first information, the client user interface comprising an icon having a position, an initial appearance, and an initial function; and changing the appearance of the icon from its initial appearance and changing the function of the icon from its initial function, while leaving the position of the icon unchanged, in response to an output becoming available in response to the first information.

12. The method of claim **11**, wherein:

the client program controls a second web browser operating independently of the first web browser to provide the separate client user interface, the client program operating without intervention from the user to provide the outputs to the user through the second web browser.

13. The method of claim **12**, wherein:

the client program is a thin shell in which the second web browser is embedded.

14. The method of claim **11**, wherein:

the client program monitors the position of a first window of the first web browser on a display and places a client window relative to the first window on the display.

15. The method of claim **11**, wherein:

the client program provides a user interface for each of one or more computer program tools, each of the tools being implemented in a computer program running on a server computer separate from the user computer, each of the tools being operable to communicate outputs to the client program.

16. The method of claim **15**, wherein:

any one or more of the computer program tools can be active at any one time; and

the user interface for each active tool comprises a client tool window, the client tool windows of the active tools being updated by the active tools as the users browses the web using the first web browser.

17. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

at least one of the tools is operable to read, and provide output based on, content of the current web page.

18. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise a speech data stream derived by a text-to-speech computer program tool from content of the current web page.

19. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise a translation from a native language of the current web page to another language.

20. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise source HTML code of the current web page.

21. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise a discussion related to content of the current web page.

22. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise a third-party comment on the current web page.

23. The method of claim **15**, wherein:

the first information from the first browser identifies a current web page; and

the outputs comprise shopping information for products of a kind shown in the current web page.

24. The method of claim **23**, wherein the shopping information comprises price and feature comparisons.

25. The method of claim **23**, wherein the shopping information comprises links to vendor web sites.

26. The method of claim **11**, wherein:

the first information from the first browser identifies a current web page, the current web page being part of a web site of a particular company; and

the outputs comprise information about the particular company.

27. A system for providing information to a user browsing the web, comprising:

means for presenting to the user one or more application tools that the user may enable and disable;

means for transmitting a context defined by the user's browsing activity to a user-selected and enabled application tool;

means for generating a web page parallel to the actual web page being visited by the user, wherein generating the web page includes running the application tool to generate a reaction to the context for the user; and

means for displaying the parallel web page.

28. A computer program product, tangibly stored on a computer-readable medium, for providing information to a user browsing the web, comprising instructions operable to cause a programmable processor to:

present to the user one or more application tools that the user may enable and disable;

transmit a context defined by the user's browsing activity to a user-selected and enabled application tool;

generate a web page parallel to the actual web page being visited by the user, including instructions to run the application tool to generate a reaction to the context for the user; and

display the parallel web page.

* * * * *

US006192380B1

(12) **United States Patent**
Light et al.

(10) **Patent No.: US 6,192,380 B1**
(45) **Date of Patent: Feb. 20, 2001**

(54) **AUTOMATIC WEB BASED FORM FILL-IN**

(75) Inventors: **John Light**, Hillsboro; **John Garney**, Aloha, both of OR (US)

(73) Assignee: **Intel Corporation**, Santa Clara, CA (US)

(*) Notice: Under 35 U.S.C. 154(b), the term of this patent shall be extended for 0 days.

(21) Appl. No.: **09/052,902**

(22) Filed: **Mar. 31, 1998**

(51) **Int. Cl.**[7] **G06F 7/06**

(52) **U.S. Cl.** **707/505**; 707/506; 707/507; 707/508; 707/9; 707/10

(58) **Field of Search** 707/505, 506, 707/507, 508, 9, 10

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,640,577 * 6/1997 Scharmer 395/768
5,794,259 * 11/1998 Kikinis 707/507
5,802,518 * 9/1998 Karaev et al. 707/9
5,931,907 * 8/1999 Davies et al. 709/218
5,963,952 * 5/1999 Smith 707/102
5,974,430 * 10/1999 Mutschler 707/505
6,029,245 * 2/2000 Scanlan 713/200

OTHER PUBLICATIONS

Laura Lemay's Teach Yourself Web Publishing with HTML 3.2. pp. 555,560,561,562,757. Copyright 1996 by Sams.net Publishing, 1996.*

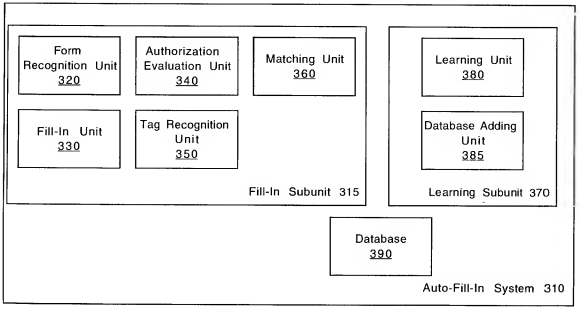
* cited by examiner

Primary Examiner—Thomas G. Black
Assistant Examiner—Thuy Do
(74) *Attorney, Agent, or Firm*—Blakely, Sokoloff, Taylor & Zafman LLP

(57) **ABSTRACT**

A method and apparatus for automatic web form fill-in is provided. A web page is accessed. A form included in the web page is recognized. Data is automatically filled into the form from a database.

19 Claims, 7 Drawing Sheets



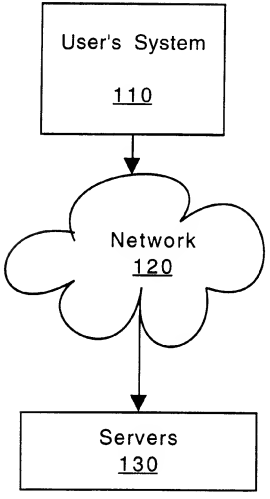


Fig. 1

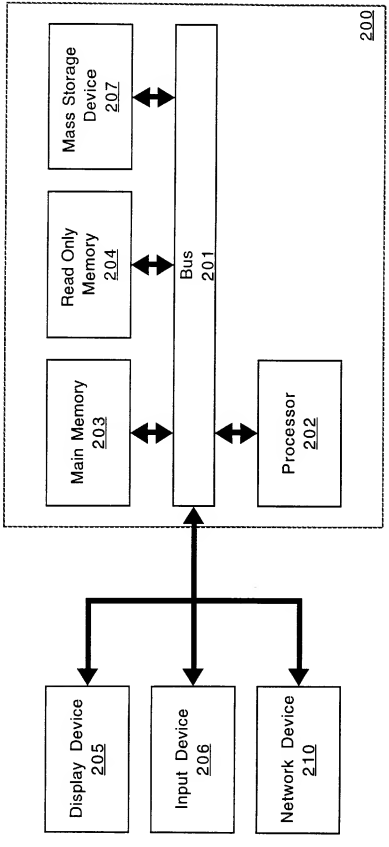

200
Mass Storage Device 207
Read Only Memory 204
Bus 201
Main Memory 203
Processor 202
Display Device 205
Input Device 206
Network Device 210

Fig. 2

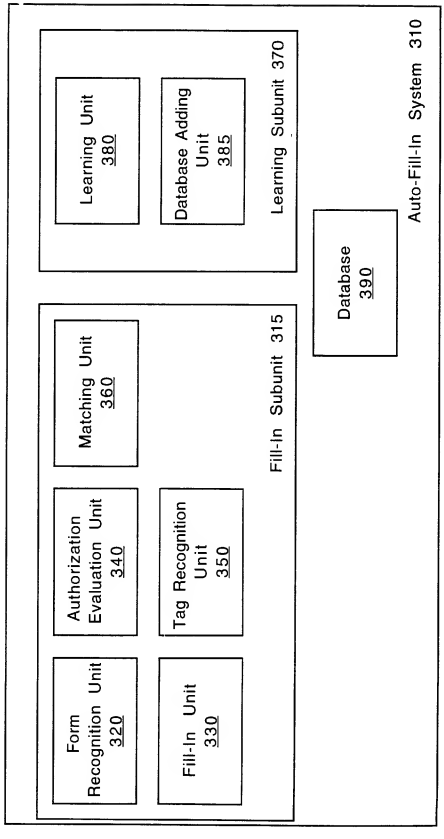

Auto-Fill-In System 310
Learning Subunit 370
Learning Unit 380
Database Adding Unit 385
Database 390
Fill-In Subunit 315
Form Recognition Unit 320
Fill-In Unit 330
Authorization Evaluation Unit 340
Tag Recognition Unit 350
Matching Unit 360

Fig. 3

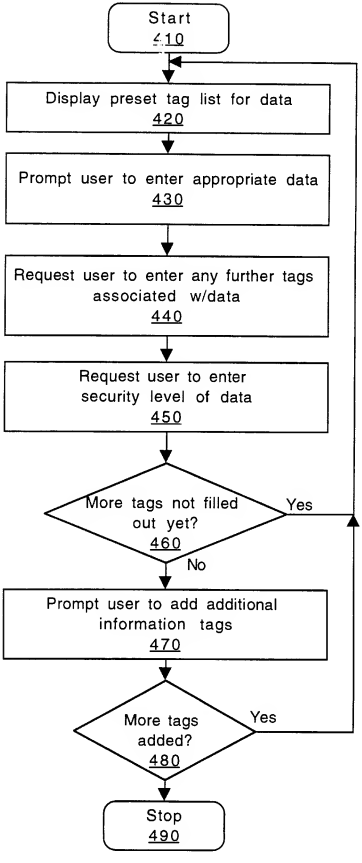

Start
410
Display preset tag list for data
420
Prompt user to enter appropriate data
430
Request user to enter any further tags associated w/data
440
Request user to enter security level of data
450
More tags not filled out yet?
460
Yes
No
Prompt user to add additional information tags
470
More tags added?
480
Yes
Stop
490

Fig. 4

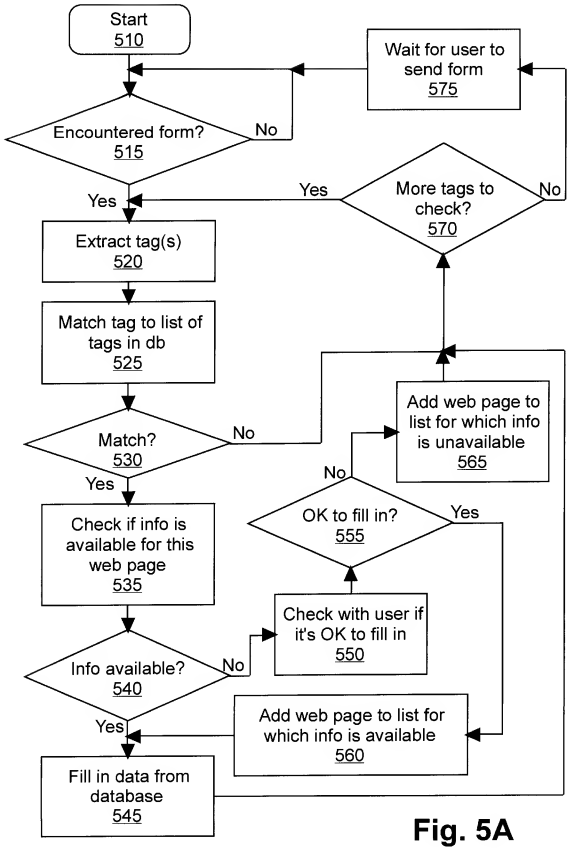

Start
510
Wait for user to send form
575
Encountered form?
515
No
Yes
Yes
More tags to check?
570
No
Extract tag(s)
520
Match tag to list of tags in db
525
Add web page to list for which info is unavailable
565
Match?
530
No
Yes
No
OK to fill in?
555
Yes
Check if info is available for this web page
535
Check with user if it's OK to fill in
550
Info available?
540
No
Yes
Add web page to list for which info is available
560
Fill in data from database
545

Fig. 5A

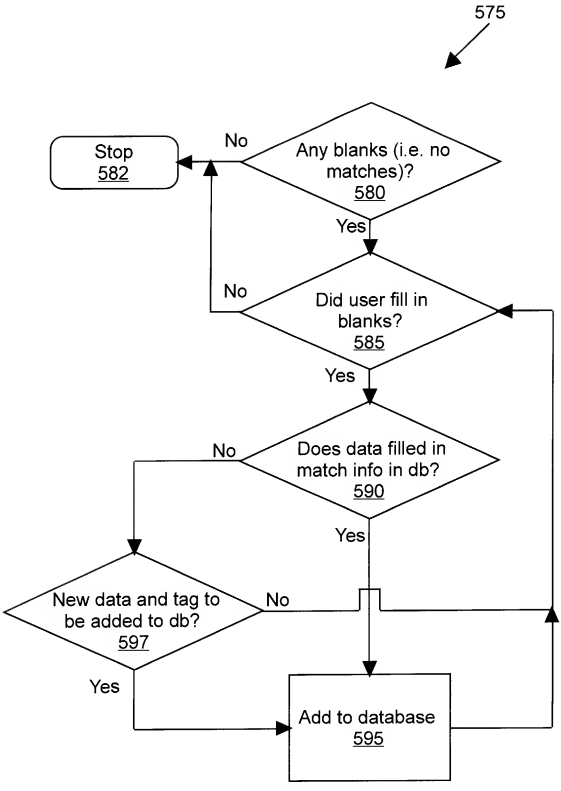

575
Stop
582
No
Any blanks (i.e. no matches)?
580
Yes
No
Did user fill in blanks?
585
Yes
No
Does data filled in match info in db?
590
Yes
New data and tag to be added to db?
597
No
Yes
Add to database
595

Fig. 5B

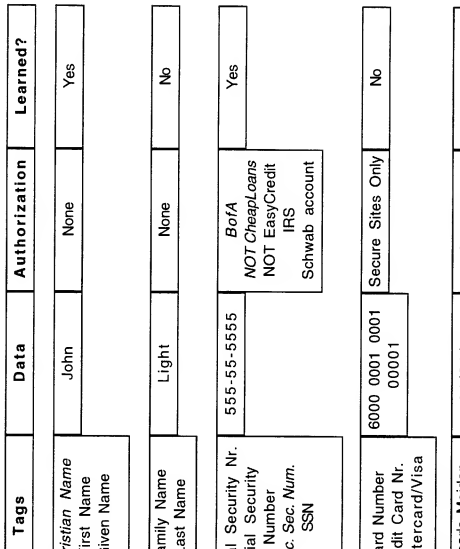

Tags
Data
Authorization
Learned?
Christian Name
First Name
Given Name
John
None
Yes
Family Name
Last Name
Light
None
No
Social Security Nr.
Social Security Number
Soc. Sec. Num.
SSN
555-55-5555
BofA
NOT CheapLoans
NOT EasyCredit
IRS
Schwab account
Yes
Card Number
Credit Card Nr.
Mastercard/Visa
6000 0001 0001 00001
Secure Sites Only
No
Mother's Maiden Name
01/01/70
ONLY IRS
No

Fig. 6

AUTOMATIC WEB BASED FORM FILL-IN

FIELD OF THE INVENTION

The present invention relates to , and more specifically, to

BACKGROUND

The World-Wide Web (WWW, W3, the Web) is an Internet client-server hypertext distributed information retrieval system. An extensive user community has developed on the Web since its public introduction. On the Web everything (documents, menus, indices) is represented to the user as a hypertext object in hypertext markup language (HTML) format. Hypertext links refer to other documents by their universal resource locators (URLs). The client program, known as a browser, e.g. NCSA Mosaic, Netscape Navigator, runs on the user's computer and provides two basic navigation operations: to follow a link or to send a query to a server.

A variety of client and server software is freely available. Most clients and servers support "forms" which allow the user to enter arbitrary text as well as selecting options from customizable menus and on/off switches. As more business is transacted on the Web, forms are proliferating. The forms may include forms for requesting further information, for ordering items from the Web, for registering for a Web site, etc.

Currently, the user has to fill out each of these forms separately. Generally, the forms request the same types of information, i.e. name, address, telephone number, e-mail address, etc. The user has to enter all of this information for each form. This is repetitious and takes time. Additionally, if such information as credit card number or social security number is requested, the user has to pull out the credit card and copy a long string of numbers. This makes errors likely. Furthermore, the user has to verify that a Web site that requests a credit card number or similar information generally kept confidential, is of the appropriate level of security for the user to feel comfortable sending the information over the Web.

SUMMARY OF THE INVENTION

A method for filling in forms in a web page is described. A web page is accessed. A form included in the web page is recognized. Data is automatically filled into the form from a database.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention is illustrated by way of example, and not by way of limitation, in the figures of the accompanying drawings and in which like reference numerals refer to similar elements and in which:

FIG. **1** is one embodiment of a network on which the present invention may be implemented.

FIG. **2** is one embodiment of a computer system on which the present invention may bc implemented.

FIG. **3** is a block diagram illustrating one embodiment of the present invention.

FIG. **4** is a flowchart illustrating one embodiment of the initial setup of the present invention.

FIG. **5**A is a flowchart illustrating one embodiment of the fill-in process.

FIG. **5**B is a flowchart illustrating the learning process associated with the fill-in process of FIG. **5**A.

FIG. **6** illustrates sample database entries.

DETAILED DESCRIPTION

A method and apparatus for automatic web form fill-in is described.

FIG. **1** is one embodiment of a network on which the present invention may be implemented. The user's system, a client, **110** is coupled to a network **120**. The client **110** may be coupled to the network **120** via a modem connection, an Ethernet connection, a local area network (LAN), a wide area network (WAN), or any other type of network connection. Servers **130** are coupled to the network **120**. For one embodiment, the server **130** may be the same computer as the client **110**. For one embodiment, these servers **130** provide Web pages to the user via the network **120**. These Web pages may include forms, as will be discussed below.

FIG. **2** is one embodiment of a computer system on which the present invention may be implemented. FIG. **2** is a block diagram of the computer system **200** in which an embodiment of the present invention can be implemented. Computer system **200** comprises a bus **201** or other communication means for communicating information, and a processor **202** coupled with bus **201** for processing information. Computer system **200** also comprises a read only memory (ROM) and/or other static storage device **204** coupled to bus **201** for storing static information and instructions for processor **202**.

The computer system **200** further comprises a main memory **203**, a dynamic storage device for storing information and instructions to be executed. Main memory **203** also may be used for storing temporary variables or other intermediate information during execution of instructions. In one embodiment the main memory **203** is dynamic random access memory (DRAM).

Computer system **200** can also be coupled to a display device **205**, such as a cathode ray tube (CRT) or liquid crystal display (LCD) screen, for displaying information to a computer user. An alphanumeric input device **206** is typically coupled to the computer system **200** for communicating information and command selections to processor **202**. The input device **206** may be a cursor control device **206**, such as a mouse, a trackball, trackpad, or cursor direction keys for communicating direction information and command selections to processor **202**, and for controlling cursor movement on display device **205**. Alternatively, other input devices **206** such as a stylus or pen can be used to interact with the display. Multiple input devices **206** may be coupled to the computer system **200**.

The computer system **200** may further be coupled to a network device **210**. The network device **210** may be a modem, an Ethernet link, or similar device for connecting the computer system **200** to a network.

FIG. **3** is a block diagram illustrating one embodiment of the present invention. For one embodiment, the present invention is part of a browser. A browser is a program which allows a person to read hypertext. The browser gives some means of viewing the contents of web pages (or nodes) and of navigating from one node to another. For an alternative embodiment, the present invention is not part of a browser, but rather an independent software unit, that interacts with the browser. The browser receives a web address from the user, and opens the corresponding web page.

The auto-fill-in system **310** includes a fill-in subunit **315** and a learning subunit **370**. The fill-in subunit **315** includes a form recognition unit **320**. When a form is included in the web page the form recognition unit **320** notes that there is a form. For one embodiment, the form includes an hypertext

markup language (HTML) tag such as "form", or "input type" indicating that it is a form or that it requires user input. The auto-fill-in system **310** then inspects the source code for the page, and recognizes tags associated with blank spaces in the form. For example, a form may look as follows:

We encourage you to enter your credit card number on-line, this is why it's secure. However, you also have the option of phoning us with the number.

Please enter your e-mail address: [ ]

My password is: [ ]

Have you forgotten your password?

My credit card type is: ○ MC ○ Visa ○ AmEx

My credit card number is: [ ]

The source code of the form may look as follows:

<form method=POST action=/exec/obidos/order-form-page1/6474-2122890-104042>

We encourage you to enter your credit card number online (<fontsize="-1">why this is safe). However, you also have the option of phoning us with the number.

<blockquote>

Please enter your e-mail address:

<input type=text name=email size=40 value="">

My password is <input type="password" size="20"name="password" maxlength=20>.

Have you forgotten your password?<p>

Credit card type

<input type=radio name=creditcardtype=MC>

<input type=radio name=creditcardtype=Visa>

<input type=radio name=creditcardtype=AmEx>

My credit card number is <input type="cardnumber" size="16" name="cardnumber" maxlength=24>.

</blockquote>

The form recognition unit **320** recognizes tags such as "input type" that connote forms. The form recognition unit **320** then passes the entire source of the web page to the tag recognition unit.

The tag recognition unit **350** then scans the form, and determines what the form is asking for. Thus, for example, in this instance, the name of the first item is "email". Alternately, the tag recognition unit **350** may recognize the label displayed to the user for the specified entry. Thus, for example the text "please enter your e-mail address" may be recognized by the tag recognition unit **350**, and "e-mail address" extracted from it. For one embodiment, the displayed label or the "name" associated with the blank is the tag recognized by the tag recognition unit **350**. For one embodiment, the name associated with the blank is the preferred tag.

Once the tag recognition unit **350** has extracted a tag, it passes the tag to the matching unit **360**. The matching unit **360** searches in the database **390** for a similar tag. For one embodiment, the matching unit **360** has some intelligence, and corrects singulars v. plurals, misspellings, words that were combined into a single word, etc. Some of the entries in the database are illustrated in FIG. **6**. The matching unit **360** determines whether there is a tag that is "email" or "e-mail address". If the matching unit **360** finds a matching tag in the database **390**, it passes the tag, the data associated with the tag, and the authorization of the tag to the authorization evaluation unit **340**.

The authorization evaluation unit **340** determines whether there are any restrictions on the data. Such restrictions may include restricting the data to only specific sites, or only secure sites, and similar restrictions. The authorization evaluation unit **340** compares the web page with the authorization data associated with the information. If the web page is authorized to receive the data, the authorization evaluation unit **340** passes the data to the filling unit **330**. The filling unit **330** inserts the data into the space associated with the tag.

In this way, the spaces in the form are filled in. If, for example, there are blank spaces, the auto-fill-in system **310** waits for the user to fill in any blanks. When the user presses enter, or otherwise indicates that the form is completely filled in, the learning subunit **370** scans the form, and determines whether there are any spaces that were filled in by the user, not the fill-in subunit **315**. The learning subunit **370** then extracts the tags and data associated with these user-filled-in spaces, and passes them to the learning subunit **370**.

The learning subunit **370** determines whether the data already exists in the database **390**. If it does, the database adding unit **385** adds the new tag to the list of tags associated with the information in the database **390**. If the data is not in the database **390**, the database adding unit **385** adds the new data and the new tag to the database **390**.

FIG. **4** is a flowchart illustrating one embodiment of the initial setup of the present invention. Generally, the user will wish to initially enter the personal information to be filled into the various forms. Alternatively, this step may be skipped, and the system may only learn from user input, as will be described below.

At block **410**, the initial setup starts. At block **420**, the existing list of tags is displayed. For example, this list of tags may include "First name", "Last Name", "e-mail address", etc. For one embodiment, this list of tags may be included with the application. Alternatively, the user may be questioned for tags initially.

At block **430**, the user is prompted to enter appropriate data for the existing tags. This may include information such as a name, e-mail address, credit card numbers, social security number, etc.

At block **440**, the user is requested to enter further tags associated with the data. Thus, for example, when the user enters his or her first name, in response to a tag asking for a "first name", the user may add other tags, such as "given name", etc.

At block **450**, the user is requested to enter the authorization level for the data. Data may be divided into multiple categories, as illustrated for example in FIG. **6**. Data may have no authorization restrictions. Information such as name and e-mail address may be generally released to all sites that ask for them.

Alternately, data may be restricted to only a certain one or list of sites. Thus, for example, for a social security number, the user may enter that the social security number may be released to the IRS, to the user's bank, etc. The user may further specify locations to which the information should not be released. Thus, for example, if there is page that is regularly visited that the user does not wish to release the data to, negative authorizations may also be entered.

A second type of authorization includes exclusive authorization. This is illustrated in FIG. **6** as well. The entry

tagged "mother's maiden name" which is often used by credit card companies for identification, may be restricted to be released only to the IRS. An authorization restricted as exclusive may include a list of one or more locations to which the data may be provided. When the user encounters a form that asks for data restricted by exclusive authorization, i.e. a page that asks for the user's mother's maiden name, the system does not query whether the user wishes to fill in the information. Rather, if the site is not in the list of sites, the system does not fill in the information, and assumes that the user will not release the information.

A third type of authorization is "secure site" authorization. Secure site authorization may include sites that have a verified certification from a recognizes certification authority, this may include encrypted sites, or otherwise secured sites. The security level may be set by the user. For one embodiment, all sites running secure hypertext transmission protocol (https) or a secure sockets layer (SSL) are deemed secure sites. Alternative authorization levels may be included, or may be defined by the user.

At block **460**, the system tests whether there are any blank tags remaining. The user may indicate that he or she does not wish to enter data for a preexisting tag. In that instance, the data associated with that tag is set to null, but not considered a blank tag for the purposes of the preliminary entry of data.

If there are blank tags, the system loops back to block **420**, and displays the tag list that has not been completed. If there are no blank tags, the system continues to block **470**.

At block **470**, the user is prompted to add additional tags. The user may, for instance, often use a system that requires age information. Thus, the user may add "age" as a tag, and fill in his or her age as data. At block **480**, the system tests whether more tags have been added. If more tags were added, the system returns to block **420**, and displays the added tags to the user for authorization level, etc. If no more tags were added by the user at block **470**, the preliminary data gathering is ended, and the flowchart stops at block **490**.

FIG. **5**A is a flowchart illustrating one embodiment of the fill-in process. The process starts at block **510**. At block **515**, the process tests whether a form has been encountered. If no form has been encountered, the process returns to block **515**. For one embodiment, this process is activated every time a new web page is opened. For one embodiment, the process runs in the background. If no forms were found at block **515**, the process returns to the background state, at block **510**. If a form is found, the process continues to block **520**. Alternatively, the fill-in process may be activated by the user. For one embodiment, the user may activate the fill-in process by pressing a key, a key combination, a left mouse button, or a similar activation mechanism.

At block **520**, a tag is copied. Each form has at least one entry blank to be filled in by the user. A least one tag is associated with every entry blank, indicating what the user should enter into the form. For one embodiment, the name of the input is copied as a tag. Thus, in the example above, the name "cardnumber" may be copied as a tag. For another embodiment, a displayed label associated with the entry blank may be copied. Thus, the text "My credit card number is:" is copied, and the tag "credit card number" is extracted from the text. For another embodiment, both the displayed label and the name are extracted as tags.

At block **525**, the tag is matched to a list of tags in the database. The database includes all of the tags originally supplied, tags entered by the user, and tags learned, as will be discussed later. The extracted tag is compared to the tags in the database.

At block **530**, the process tests whether there was a match between the extracted tag and the list of tags in the database. If there is no match, the process goes to block **570**. At block **570**, the process tests whether there are any more tags to check. If there are tags remaining to be checked, the process returns to block **520**. If there are no remaining tags to be checked, the process continues to block **575**, and the process waits for the user to send the form. If, at block **530**, a match was found, the process continues to block **535**.

At block **535**, the process tests whether the data associated with the matching tag found in the database is available for this web page. As discussed above, there are various levels of authorization for data. Thus, at block **535**, the process tests whether the data is authorized to be released to the web page in question.

At block **540**, the process determines whether or not the data is available. If the data is available, the process continues to block **545**. At block **545**, the data is filled into the form. The process then continues to block **570**, where it tests whether there are any more tags to check.

If, at block **540**, it is determined that the data is not available, the process continues to block **550**. For one embodiment, the process collects all of the data that is not properly authorized, and tests authorization for all of the data at the same time. In other words, only after no blank spaces remain does the process continue to block **550**.

At block **550**, the user is queried whether it is acceptable to fill-in the data. For one embodiment, the user is queried only if the authorization level is not set to exclusive authorization. For another embodiment, the user is not queried if the page is on the exclusion list, as described above.

At block **555**, it is tested whether it is acceptable to fill-in the data. If it is acceptable to fill-in the data, the process continues to block **560**. At block **560**, the web page is added to the list of authorized sites for which the data is available. The process then continue to block **545**.

At block **555**, if it is determined that it is not acceptable to enter the data, the process continues to block **565**. At block **565**, the web page is added as a negative authorization That is, if this web site is encountered in the future, the user is not queried whether the data is available, but rather, the blanks are automatically left blank. From block **565**, the process returns to block **570**, and queries whether there are more tags to check.

FIG. **5**B is a flowchart illustrating the learning process associated with the fill-in process of FIG. **5**A. In FIG. **5**A, the blanks are automatically filled by the system. When the last blank is filled in, the system waits for the user to send the form, at block **575**. However, the user may enter additional data prior to sending the form. FIG. **5**B illustrates the process occurring concurrently with, or after, waiting for the user to send the form, at block **575** of FIG. **5**A.

Returning to FIG. **5**B, at block **580**, the system tests if there are any blanks, i.e. areas which the automatic fill-in did not complete. If there are no blanks, the learning process is finished. If there are blanks, the system, at block **585**, tests whether the user filled in any of the blanks. In many forms, areas may be left blank. Thus, the user may not chose to complete every entry on the form. If, at block **585**, the process finds that the user did not fill in any blanks, the learning process is finished. If the user filled in at least one blank, the process continues to block **590**.

At block **590**, the system queries whether the data filled in matches information in the database. This is applicable if a different tag is used by the web page for known data. For example, the tag "Christian name" may be used in a foreign web page, for the data tagged "first name" in the database. The data entered by the user would still be "John", or the appropriate first name.

If the data matches information in the database, the process continues to block **595**. At block **595**, the new tag is added to the list of tags associated with the information found in the database. Thus, the tag "Christian name" would be added to the tags associated with the data "John" in the above example. The process then returns to block **585**, to query whether any other blanks were filled in by the user.

If, at block **590**, it is found that the data does not match information in the database, the process continues to block **597**.

At block **597**, the user is queried whether the new data should be added to the database. If the user replies in the negative, the process returns to block **585**, and the system again queries whether any other blanks were filled in by the user. If the user replies in the affirmative, the process continues to block **595**. At block **595**, the new tag and new data associated with it are added to the database. For another embodiment, the tag and data are automatically added to the database.

FIG. **6** illustrates sample database entries, as discussed above. Other data may of course be included in the database. Alternative arrangements of data may include not having an authorization, not having an indicator whether anything in the list was learned, etc.

In the foregoing specification, the invention has been described with reference to specific exemplary embodiments thereof. It will, however, be evident that various modifications and changes may be made thereto without departing from the broader spirit and scope of the invention as set forth in the appended claims. The specification and drawings are, accordingly, to be regarded in an illustrative rather than a restrictive sense.

What is claimed is:

1. A method comprising:

recognizing a form in a web page;

identifying information to be filled into the form;

determining whether data corresponding to the information to be filled into the form is authorized by a user to be disclosed to the web page;

automatically filling the data into the form from a database if the data is authorized by the user to be disclosed to the web page.

2. The method of claim **1**, wherein recognizing the form further comprises extracting tags from the web page.

3. The method of claim **2**, wherein recognizing the form further comprises:

comparing the tags with a stored tag list in the database;

identifying a matched tag; and

inserting the data corresponding to the matched tag into the form.

4. The method of claim **3**, wherein determining whether the data corresponding to the information to be filled into the form is authorized to be disclosed to the web page comprises:

determining an authorization of the data; and

comparing the authorization of the data with an authorization level of the web page.

5. The method of claim **4**, further comprising:

if the web page is not authorized for the data, prompting the user to decide whether the web page should be authorized for the data; and

if the user decides that the web page should be authorized for the data, inserting the data and adding the web page to a list of authorized web pages for the data.

6. The method of claim **5** further comprising, if the user decides that the web page should not be authorized for the data, adding the web page to a list of not authorized web pages for the data.

7. The method of claim **1**, further comprising:

determining if the user filled additional data into blank fields in the form;

if the user did fill additional data into blank fields in the form, determining if the additional data corresponds to data already stored in the database; and

if the additional data corresponds to data already stored in the database, adding a tag associated with the additional data to a list of tags associated with the data already stored in the database.

8. The method of claim **7**, further comprising:

determining if the list of tags has an authorization list; and

if the list of tags has an authorization list, adding the web page on which the blank field was found to the authorization list for the data already stored in the database.

9. The method of claim **7**, further comprising:

determining if the additional data does not correspond to the stored data;

if the additional data does not correspond to the stored data, storing the additional data and the tag associated with the additional data in the database.

10. The method of claim **9**, further comprising automatically authorizing the additional data for the web page on which the blank fields were found.

11. The method of claim **9**, further comprising prompting the user to enter a security level for the additional data entered into the blank fields.

12. A method comprising:

opening a web page;

recognizing a form in the web page;

extracting tags from the form in the web page;

comparing the tags with a stored tag list in the database;

identifying a matched tag in the database;

determining whether the web page is authorized for the data corresponding to the matched tag;

if the web page is authorized for the data, inserting the data into the form in the web page; and

if the web page is not authorized for the data:

prompting a user to decide whether the web page should be authorized for the data;

if the user decides that the web page should be authorized for the data:

inserting the data into the form; and

adding the web page to a list of authorized web pages for the data; and

if the user decides that the web page should not be authorized for the data, adding the web page to a list of unauthorized web pages for the data.

13. A system comprising:

a plurality of personal data, tags, and an authorization level associated with the personal data;

a form recognition unit for recognizing information requested by a form in a web page;

an authorization evaluation unit for determining the authorization level of the personal data corresponding to the information requested by the form, and for determining an authorization level of the web page; and

a fill-in unit for filling the personal data from the database into the form, if the authorization evaluation unit authorizes the personal data for the web page.

14. The system of claim **13**, further comprising a tag extraction logic for extracting tags from the form in the web page.

15. The system of claim 15, further comprising:

a matching unit for comparing the tags extracted from the form with a stored tag list in the database and identifying a matched tag; and

wherein said fill-in unit receives the personal data from the matching unit if the matched tag is found.

16. The system of claim 16, wherein the authorization evaluation unit authorizes the matching unit to pass the personal data to the fill-in unit if the web page is authorized for the personal data.

17. The system of claim 17, wherein the authorization evaluation unit determines whether the web page should be authorized for the data and, if the web page should be authorized for the data, inserts the data and adds the web page to a list of authorized web pages for the data.

18. The system of claim 13, further comprising:

a learning subunit for adding personal data to the database, the personal data being entered by a user and not having been previously included in the database.

19. A method comprising:

opening a web page;

recognizing a form in a web page;

extracting tags from the web page;

comparing the tags with a stored tag list in a database;

identifying a matched tag;

determining whether data corresponding to the matched tag is authorized to be disclosed to non-listed sites;

prompting a user to decide if the web page should be authorized for the data, if the data is not authorized to be disclosed to non-listed sites; and

inserting the data corresponding to the matched tag into the form, if the user decides that the web page should be authorized for the data, or if the data is authorized to be disclosed to non-listed sites.

* * * * *

US005930767A

United States Patent [19]

Reber et al.

[11] Patent Number: 5,930,767

[45] Date of Patent: Jul. 27, 1999

[54] **TRANSACTION METHODS SYSTEMS AND DEVICES**

[75] Inventors: **William Louis Reber**, Schaumburg, Ill.; **Cary Drake Perttunen**, Shelby Township, Mich.

[73] Assignee: **Motorola, Inc.**, Schaumburg, Ill.

[21] Appl. No.: **08/858,184**

[22] Filed: **May 28, 1997**

[51] **Int. Cl.**[6] **G06F 17/00**

[52] **U.S. Cl.** **705/26**; 380/24; 380/25; 380/23

[58] **Field of Search** 705/26, 44, 39; 380/24, 25, 4, 52, 49, 23; 395/200.33, 200.47, 200.49

[56] **References Cited**

U.S. PATENT DOCUMENTS

3,668,312	6/1972	Yamamoto et al.	348/17
3,868,514	2/1975	Israelsson	250/566
4,031,358	6/1977	Thorniley	235/472.03
4,465,926	8/1984	Apitz et al.	235/462.49
4,599,489	7/1986	Cargille	380/4
4,621,259	11/1986	Schepers et al.	345/180
4,720,860	1/1988	Weiss	380/23
4,816,904	3/1989	McKenna et al.	348/13
4,841,132	6/1989	Kajitani et al.	235/462.46
4,926,255	5/1990	Von Kohorn	348/13
4,947,028	8/1990	Gorog	235/380
5,168,520	12/1992	Weiss	380/23
5,180,192	1/1993	Herbert	283/101
5,247,347	9/1993	Litteral et al.	348/7
5,249,044	9/1993	Von Kohorn	348/12
5,287,181	2/1994	Holman	348/473
5,319,454	6/1994	Schutte	348/5.5
5,357,276	10/1994	Banker et al.	348/7
5,438,355	8/1995	Palmer	348/1
5,446,490	8/1995	Blahut et al.	348/7
5,450,491	9/1995	McNair	380/25
5,483,052	1/1996	Smith, III et al.	235/462.49
5,515,270	5/1996	Weinblatt	705/14
5,570,412	10/1996	LeBlanc	455/456
5,640,193	6/1997	Wellner	348/7
5,715,314	2/1998	Payne et al.	380/24
5,729,594	3/1998	Klingman	379/93.12
5,748,740	5/1998	Curry et al.	380/25
5,815,577	9/1998	Clark	380/52
5,826,241	10/1998	Stein et al.	705/26
5,832,119	11/1998	Rhoads	382/232

OTHER PUBLICATIONS

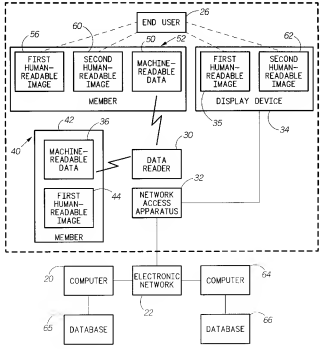
USA Today, Friday Jan. 24, 1997, p. 3A, and several pages of Internet content.

Primary Examiner—James P. Trammell
Assistant Examiner—Demetra R. Smith

[57] **ABSTRACT**

A transaction system includes a computer (**20**) which performs a transaction method comprising steps of receiving a first data element indicating an item in a transaction, receiving a second data element indicating a party of the transaction, approving the transaction based upon the second data, and creating a record of the transaction. The first data element and the second data element are received via an electronic network (**22**). The second data element is read from a device (**40**) by an optical data reader (**30**) in communication with the electronic network (**22**).

23 Claims, 5 Drawing Sheets



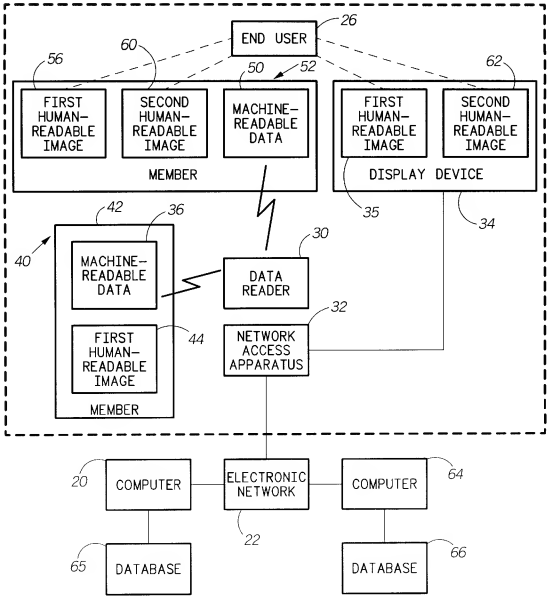

END USER
26
60
56
50
52
62
FIRST HUMAN–READABLE IMAGE
SECOND HUMAN–READABLE IMAGE
MACHINE–READABLE DATA
MEMBER
FIRST HUMAN–READABLE IMAGE
SECOND HUMAN–READABLE IMAGE
DISPLAY DEVICE
35
34
42
36
40
30
MACHINE–READABLE DATA
DATA READER
32
FIRST HUMAN–READABLE IMAGE
44
NETWORK ACCESS APPARATUS
MEMBER
20
COMPUTER
ELECTRONIC NETWORK
COMPUTER
64
22
65
DATABASE
DATABASE
66

FIG. 1

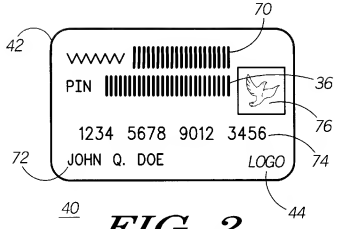


FIG. 2

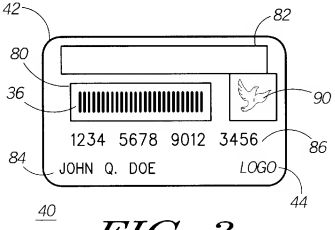


FIG. 3

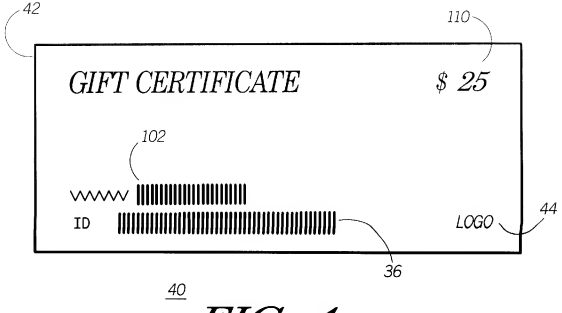


FIG. 4

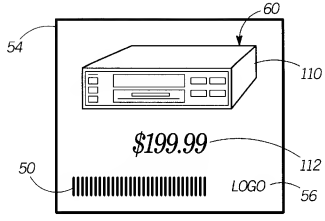


FIG. 5

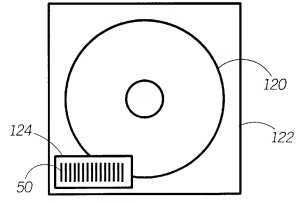


FIG. 6

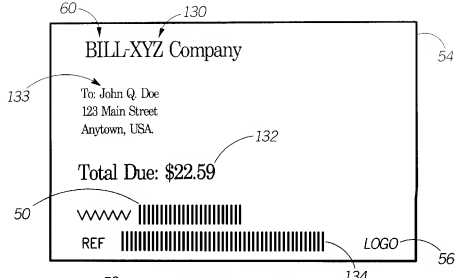


FIG. 7

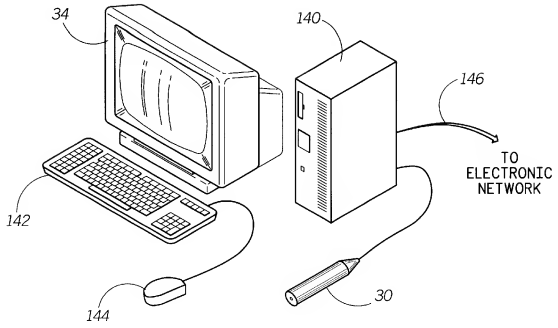

34
140
146
TO
ELECTRONIC
NETWORK
142
144
30

FIG. 8

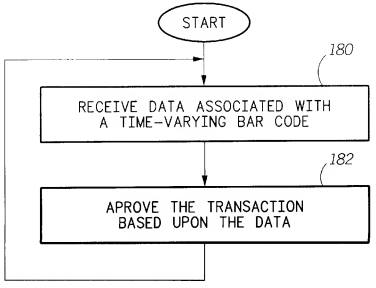

START
180
RECEIVE DATA ASSOCIATED WITH
A TIME-VARYING BAR CODE
182
APROVE THE TRANSACTION
BASED UPON THE DATA

FIG. 11

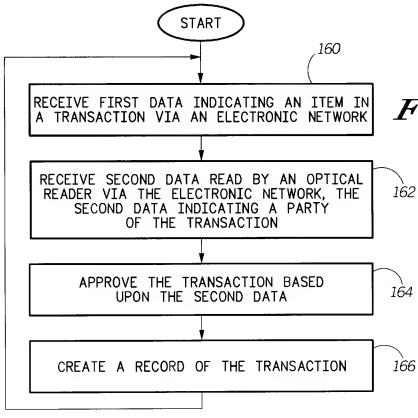

START
160
RECEIVE FIRST DATA INDICATING AN ITEM IN A TRANSACTION VIA AN ELECTRONIC NETWORK
RECEIVE SECOND DATA READ BY AN OPTICAL READER VIA THE ELECTRONIC NETWORK, THE SECOND DATA INDICATING A PARTY OF THE TRANSACTION
162
APPROVE THE TRANSACTION BASED UPON THE SECOND DATA
164
CREATE A RECORD OF THE TRANSACTION
166

FIG. 9

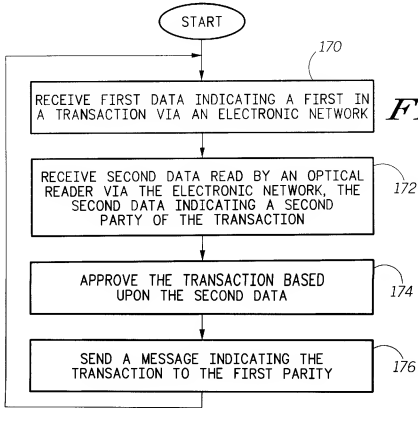

START
170
RECEIVE FIRST DATA INDICATING A FIRST IN A TRANSACTION VIA AN ELECTRONIC NETWORK
RECEIVE SECOND DATA READ BY AN OPTICAL READER VIA THE ELECTRONIC NETWORK, THE SECOND DATA INDICATING A SECOND PARTY OF THE TRANSACTION
172
APPROVE THE TRANSACTION BASED UPON THE SECOND DATA
174
SEND A MESSAGE INDICATING THE TRANSACTION TO THE FIRST PARITY
176

FIG. 10

TRANSACTION METHODS SYSTEMS AND DEVICES

RELATED APPLICATIONS

The present application is related to the following applications:

"Electronic Network Navigation Device and Method for Linking to an Electronic Address Therewith", having Ser. No. 08/710,810, filed Sep. 23, 1996;

"Methods and Systems for Providing a Resource in an Electronic Network", having Ser. No. 08/726,004, filed Oct. 4, 1996;

"An Apparatus for Reading an Electronic Network Navigation Device and a Peripheral for Use Therewith", having Serial No. 08/732,956, filed Oct. 17, 1996;

"Method, System, and Article of Manufacture for Producing a Network Navigation Device", having Ser. No. 08/744,338, filed Nov. 7, 1996; and

"Bar Code Display Apparatus", having Docket No. MNE00510, filed May 28, 1997.

The subject matter of the above-identified related applications is hereby incorporated by reference into the disclosure of this application.

TECHNICAL FIELD

The present invention relates to methods, systems, and devices for performing transactions via an electronic network such as the Internet.

BACKGROUND OF THE INVENTION

Many companies have proposed services for selling products on the Internet. One such service involves offering software tools to create, host, and manage a Web site and a Web-based store to perform transactions over the Internet.

Included in the service is support for credit card purchases over the Internet. When an end user registers for the service, he/she is assigned a personal identification number as a proxy for his/her credit card number. To make a purchase over the Internet, the end user enters the personal identification number into his/her personal computer. The personal computer, in turn, communicates the personal identification number to a Web-based merchant via the Internet. The purchase is made based on the personal identification number rather than a credit card number.

Advantageously, the use of the personal identification number prevents an interception of the end user's credit card number by unauthorized parties. A drawback of using a personal identification number is that many individuals currently have other personal identification numbers and passwords to remember. Additionally, the interception of the end user's personal identification number can result in transactions by unauthorized parties. Accordingly, there is a need for improved methods, systems, and devices for Internet transactions.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention is pointed out with particularity in the appended claims. However, other features of the invention will become more apparent by referring to the following detailed description in conjunction with the accompanying drawings in which:

FIG. **1** is a block diagram of an embodiment of a transaction system in accordance with the present invention;

FIG. **2** is a view of a first example of the device **40** described with reference to FIG. **1**;

FIG. **3** is a view of a second example of the device **40** described with reference to FIG. **1**;

FIG. **4** is a view of a third example of the device **40** described with reference to FIG. **1**;

FIG. **5** is a view of a first example of the device **52** described with reference to FIG. **1**;

FIG. **6** is a view of a second example of the device **52** described with reference to FIG. **1**;

FIG. **7** is a view of a third example of the device **52** described with reference to FIG. **1**;

FIG. **8** is an illustration of an example of the data reader and the network access apparatus at the user location;

FIG. **9** is a flow chart summarizing steps performed in an embodiment of a transaction method;

FIG. **10** is a flow chart summarizing steps performed in another embodiment of a transaction method; and

FIG. **11** is a flow chart summarizing steps performed in an embodiment of an authentication method in accordance with the present invention.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Using embodiments of the present invention, an end user is authenticated in a transaction based upon machine-readable data read by a data reader at the end user's location. Preferably, the machine-readable data includes a bar code that may be read by an optical data reader such as a bar code reader. To reduce the likelihood of unauthorized interception of a personal identification code, a time-varying bar code is used to authenticate the end user.

FIG. **1** is a block diagram of an embodiment of a transaction system in accordance with the present invention. The transaction system includes a computer **20** in communication with an electronic network **22**. The computer **20** includes a server or like processing apparatus which serves as a node in the electronic network **22**.

Preferably, the electronic network **22** includes a wide area network such as the Internet, the World Wide Web, or an online service to provide accessibility to the computer **20** for a wide geographical area. Other examples of the electronic network **22** include but are not limited to: an intranet, a local area network, a telephone network such as a public switched telephone network, a cellular telephone network, a personal communication system (PCS) network, a television network such as a cable television system, a paging network such as a local paging network, a regional paging network, a national paging network, or a global paging network, and a wireless data network such as a satellite data network or a local wireless data network.

The computer **20** receives transaction data generated at a user location **24** via the electronic network **22**. Typically, the user location **24** is remotely located from the computer **20**. For example, the user location **24** can be located in another city, another state, or another country with respect to the location of the computer **20**.

In a first embodiment, the transaction data includes a first data element indicating an item in a transaction and second data element indicating a party of the transaction. The item in the transaction can include: (i) merchandise such as a product, goods, or commodities; (ii) a statement of charges such an invoice or a bill; (iii) a financial instrument such as a bond, shares of a stock, or shares of a mutual fund; (iv) derivatives such as options or futures; or (v) a service. The party of the transaction can include an end user **26** present at the user location **24**, an organization associated with the

end user **26**, an organization associated with the user location **24**, or an account associated with any of the above-listed entities.

The transaction data is generated at the user location **24** by a data reader **30** and/or a network access apparatus **32**. Preferably, the data reader **30** includes an optical data reader to read printed data or human-viewable data (which may or may not be human-readable data) associated with the transaction data. Examples of the optical data reader include, but are not limited to, an optical scanner, a page scanner, a handheld scanner, a photograph reader, a business card reader, a bar code reader, a scanning wand, a linear CCD (charge coupled device) reader, a two-dimensional CCD reader, and a fax machine.

Alternatively, the data reader **30** can include a magnetic data reader to read magnetically-stored transaction data, or an electronic data reader to read electronically-stored transaction data. Embodiments of alternative data readers are described in the above-listed applications incorporated by reference into this application.

The network access apparatus **32** facilitates communication between the data reader **30** and the electronic network **22**. The network access apparatus **32** can also serve to generate at least a portion of the transaction data, and/or to receive user-initiated events to generate at least a portion of the transaction data. The network access apparatus **32** can have a variety of forms, including but not limited to, a general purpose computer, a network computer, a network television, an Internet television, a portable wireless device, a television receiver, a game player, and a video recorder.

Regardless of its form, the network access apparatus **32** typically includes a processor in communication with at least one input device, a memory, and at least one storage device. The processor can include a microprocessor, an application specific integrated circuit, or other suitable integrated circuit. The memory can include a read-only memory and/or a random access memory in communication with the processor. The at least one input device can include a keyboard and/or a pointing device for receiving user-initiated events from the end user **26**. The at least one storage device can include a floppy disk drive, a PC card storage device, an optical drive, a DVD drive, or a hard drive to store computer-readable data.

A display device **34**, such as a monitor or a television, is responsive to the network access apparatus **32** to display visual information generated by the network access apparatus **32** and/or information communicated via the electronic network **22** (e.g. information from the computer **20**). The display device **34** can include a liquid crystal display (LCD) or a cathode ray tube (CRT) display, for example, having an array of display elements or pixels for displaying textual information and graphical information. Preferably, the visual information displayed by the display device **34** includes a first human-readable image **35** associated with a service which facilitates the transaction. The first human-readable image **35** can include a logo which identifies the service to the end user **26**.

Preferably, the data reader **30** reads machine-readable data **36** from a device **40** to generate the second data element indicating the party of the transaction. The device **40** includes a member **42** which supports the machine-readable data **36**, and optionally, a first human-readable image **44**. The first human-readable image **44** is associated with a service which facilitates the transaction. Preferably, the first-human readable image **44** includes the logo which identifies the service to the end user **26**. Examples of the device **40** are subsequently described with reference to FIGS. **2** to **4**.

Preferably, the machine-readable data **36** includes a printed code or a human-viewable code, such as a bar code, which encodes the second data element to identify the party in the transaction. The bar code can include a one-dimensional bar code or a two-dimensional bar code. Examples of one-dimensional bar codes include, but are not limited to, 3 of 9, UPC-A, UPC-E, Code 128, Codabar, MSI, Extended 3 of 9, Code 93, Extended Code 93, Industrial 2 of 5, Standard 2 of 5, Code 11, and UCC/EAN-128. Examples of two-dimensional bar codes include, but are not limited to, DataMatrix and PDF417. Although bar codes are human-viewable, they are practically unreadable by many humans.

Regardless of how the second data element is encoded by the machine-readable data **36**, it is preferred that the second data element include a personal identification code such as a personal identification number to identify the end user **26**, an organization, or an account. In an exemplary embodiment, the personal identification code is time-varying and nonpredictable by unauthorized parties.

Alternatively, the second data element is generated within the network access apparatus **32**. In this case, the second data element can be prestored in the network access apparatus **32** or can be generated by a code generator associated with the network access apparatus **32**. Preferably, the code generator generates the second data element which is time-varying and nonpredictable by unauthorized parties.

Optionally, the data reader **30** reads machine-readable data **50** from a device **52** to generate the first data element is associated with the item subject to the transaction. The device **52** includes a support member **54** which supports the machine-readable data **50**, and optionally, a first human-readable image **56** and a second human-readable image **60**.

As with the first human-readable images **35** and **44**, the first human-readable image **56** is associated with the service which facilitates the transaction. Preferably, the first human-readable image **56** includes the logo which identifies the service to the end user **26**. The first human-readable image **56** is similar to, and preferably equivalent to, the first human-readable image **35**.

The second human-readable image **60** includes an image associated with a transaction item. The second human-readable image **60** can include a graphical image of the item itself, textual information describing the item, a price associated with the item, and/or a logo for the item or for an organization associated with the item. Examples of the device **52** are subsequently described with reference to FIGS. **5** to **7**.

Alternatively, the first data element is generated in response to a user-initiated event received by an input device of the network access apparatus **32**. In this case, the end user **26** can select the item and initiate a transaction based upon a second human-viewable image **62** displayed by the display device **34**. As with the second human-readable image **60**, the second human-readable image **62** can include a graphical image of the item itself, textual information describing the item, a price associated with the item, and/or a logo for the item or for an organization associated with the item. The item can be selected by a point and click operation using a pointed device or by depressing one or more keys of the network access apparatus **32**, for example.

Regardless of how the transaction data is produced, the network access apparatus **32** communicates the transaction data to the computer **20** via the electronic network **22**. Preferably, the transaction data is encrypted by the network access apparatus **32** prior to its transmission via the elec-

tronic network **22**. In this case, the computer **20** decrypts data received from the electronic network **22** to recover the transaction data.

The computer **20** selectively approves or disapproves the transaction based upon the second data element. The approval or disapproval of the transaction is based upon a step of authenticating the second data element. The second data element can be authenticated locally by the computer **20** or remotely by a computer **64**.

If done locally, the computer **20** approves the transaction by comparing the second data element and other associated data to entries in a database within or in communication with the computer **20**. Based upon the comparison, the computer **20** determines the authenticity of the transaction party. If authentic, the transaction is approved. If not authentic, the transaction is disapproved.

If authenticated remotely, the computer **20** approves the transaction by sending a first message based upon the second data element to the computer **64**. The computer **64** compares the second data element and other associated data to entries in a database associated with the computer **64**, and either accepts or rejects the authenticity of the transaction party based upon the comparison. The computer **64** sends a second message indicating either an acceptance or a rejection of the authenticity of the transaction party to the computer **20**. The computer **20** receives the second message and either approves or disapproves the transaction based thereupon.

Preferably, the computer **64** serves to authenticate transaction parties for a plurality of computers associated with the electronic network **22**. The computer **64** preferably maintains the database of personal identification codes for a plurality of accounts of end users and/or organizations.

After approving the transaction, the computer **20** creates a record of the transaction. The record of the transaction includes data representative of the date of the transaction, the time of the transaction, the party initiating the transaction, the item, a party associated with the item, and a charge amount for the transaction.

Additionally, the computer **20** can initiate an action to be performed based upon the transaction. Examples of actions include, but are not limited to, sending an item to the party, preparing an item for pick-up by the party, providing a service for the party, accounting that a bill has been paid by the party, or sending a receipt to the party.

Additionally, the herein-described transaction system can be used to perform a second preferred transaction method. In this case, the computer **64** receives transaction data via the electronic network **22**. The transaction data includes a first data element indicating a first party of a transaction and a second data element indicating a second party of the transaction. The first party includes a creditor, a seller, a merchant, a manufacturer, a payee, or other like entity which is to receive money in the transaction. The second party includes a debtor, a purchaser, a buyer, or other like entity which is to spend money in the transaction. The second party of the transaction can include an end user **26** present at the user location **24**, an organization associated with the end user **26**, an organization associated with the user location **24**, or an account associated with any of the above-listed entities.

The transfer of money from the second party to the first party can be based upon, or in return for, any of the herein-described examples of transaction items. For example, the second party may wish to purchase an item from the first party or to pay a bill from the first party.

The first data element can be generated at the user location **24** by reading the machine-readable data **50** from the device **52** using the data reader **30**. In this case, the machine-readable data **50** encodes data which identifies the first party.

Alternatively, the first data element may be generated in response to a user-initiated event received by an input device of the network access apparatus **32**. In this case, the end user **26** can select the first party based upon the second human-viewable image **62** displayed by the display device **34**. The second human-readable image **62** can include a graphical image such as a logo associated with the first party, or textual information such as a name associated with the first party. The first party can be selected by a point and click operation using a pointed device or by depressing one or more keys of the network access apparatus **32**, for example.

The second data element is generated at the user location **24** using the data reader **30** and/or the network access apparatus **32** in a manner described earlier.

The computer **64** authenticates the second data element to allow or disallow the transaction. If the second data element is authentic, the computer **64** sends a message indicating the transaction to the first party. The message can include data representative of a date of the transaction, a time of the transaction, a name associated with the second party, an address associated with the second party, an electronic address associated with the second party, the item, and a transaction amount. Optionally, the computer **64** directs that an account for the first party be credited by the transaction amount, and an account for the second party be debited by the transaction amount.

In response to receiving the message, the first party can perform an action based upon the transaction. For example, the first party can send an item to the second party, prepare an item for pick-up by the second party, provide a service to the second party, account that a bill has been paid, or send a receipt to the second party.

If the second data element is not authentic, the transaction is disallowed. In this case, the computer **64** can send a message via the electronic network **22** to the network access apparatus **32** to indicate to the end user **26** that the transaction was disallowed.

FIG. **2** is a view of a first example of the device **40** described with reference to FIG. **1**. The member **42** of the device **40** includes a substantially flat substrate formed of a dielectric or nonmagnetic material such as paper, cardboard, or plastic. The member **42** is sized for carrying within a wallet, a purse, or a pocket of the end user **26**. Preferably, the member **42** is shaped and sized as a credit card or a debit card for this purpose. Alternatively, the member **42** can have shapes and sizes of other cards, including but not limited to, a business card, a smart card, an index card, a trading card, or a playing card.

The machine-readable data **36** includes a bar code supported by the member **42**. The bar code encodes a personal identification code for the end user **26** for performing transactions over the electronic network **22**. The first human-readable image **44** includes a logo for the transaction service provided by either the computer **20** or the computer **64**.

Optionally, the member **42** further supports machine-readable data **70** for linking the network access apparatus **32** to a resource provided by the computer **64**. Preferably, the machine-readable data **70** includes a bar code encoding an electronic address such as a URL (uniform resource locator) or an IP (Internet Protocol) address. The electronic address can be for a resource or a destination (such as a Web page) associated with the service provided by the computer **64**.

The machine-readable data **70** can generally include any of the machine-readable data for network navigation devices

described in the above-listed patent application references which are incorporated by reference into the present application.

Optionally, the device **40** further serves as a credit card, a debit card, a charge card, or an automatic teller machine (AIM) card. In this case, the member **42** can further support: (i) a name **72** of a party such as the end user **26**; (ii) a card number **74** such as a credit card number, a debit card number, a charge card number, or an ATM card number associated with the party; (iii) a hologram **76** for authenticating the device **40** at a point of sale; (iv) a magnetic stripe (not illustrated) on an opposite side of the member **42**; and (v) a picture of the end user **26**. Preferably, the name **72** and the card number **74** are printed with raised letters and numerals in accordance with a standard credit card. Additionally, the support member **42** can support any other information to be disposed on a credit card or other financial card, such as a photo ID (not shown) of the end user **26**.

FIG. **3** is a view of a second example of the device **40** described with reference to FIG. **1**. The device **40** includes an embodiment of an apparatus described in the reference entitled "Bar Code Display Apparatus" which is incorporated by reference into this disclosure. In this example, the member **42** of the device **40** includes a card-shaped housing having at least one dimension, and preferably two or more dimensions, sized as a credit card or the like. The member **42** houses or supports a time-varying nonpredictable code generator (not illustrated) and a display device **80**. The time-varying nonpredictable code generator and the display device **80** are powered by either a solar battery **82**, an internal battery (not illustrated), or a plastic battery integrated with the housing.

The display device **80** is responsive to the time-varying nonpredictable code generator to display the machine-readable data **36** as a time-varying nonpredictable bar code. The time-varying nonpredictable bar code can be displayed using a one-dimensional bar code or a two-dimensional bar code such as those previously described. The bar code encodes a time-varying nonpredictable personal identification code for the end user **26** for performing transactions over the electronic network **22**.

Preferably, the time-varying nonpredictable code generator includes any of the code generators described in U.S. Pat. Nos. 4,599,489, 4,720,860, and 5,168,520 which are hereby incorporated by reference into this disclosure. Optionally, the time-varying nonpredictable code generator is synchronized to a second code generator associated with the computer **20** and/or the computer **64**. In general, the time-varying nonpredictable code generator can generate a nonpredictable code using either a random process or a pseudorandom process as described in the application entitled "Bar Code Display Apparatus".

Optionally, the display device **80** can further display a prestored bar code image for linking the network access apparatus **32** to a resource provided by the computer **64**. Preferably, the prestored bar code image includes an electronic address such as a URL (uniform resource locator) or an IP (Internet Protocol) address for a resource (such as a Web page) associated with the service provided by the computer **64**. In general, the prestored bar code image can include any of the machine-readable data for network navigation devices described in the above-listed patent application references which are incorporated by reference into this disclosure. To identify the transaction service, the first human-readable image **44** includes a logo.

As with the example of FIG. **2**, the device **40** optionally serves as a credit card, a debit card, a charge card, or an ATM card. In this case, the member **42** can further support: (i) a name **84** of a party such as the end user **26**; (ii) a card number **86** such as a credit card number, a debit card number, a charge card number, or an ATM card number associated with the party; (iii) a hologram **90** for authenticating the device **40** at a point of sale; (iv) a magnetic stripe (not illustrated) on an opposite side of the member **42**; and (v) a picture of the end user **26**. Preferably, the name **84** and the card number **86** are printed with raised letters and numerals as a standard credit card. If desired, the device **40** can have a common account for electronic network transactions and credit card, debit card, charge card, or automatic teller machine (ATM) card transactions.

FIG. **4** is a view of a third example of the device **40** described with reference to FIG. **1**. In this example, the device **40** is amenable for use in prepaid transactions. For example, the device **40** can be purchased as a gift certificate or the like to facilitate one or more prepaid transactions at a later time. The transactions can be performed by the purchaser of the device **40**, or by a recipient of the device **40**. Optionally, the device **40** can be designated only for a single use.

The support member **42** of the device **40** includes a substantially flat substrate formed of a dielectric material such as paper, cardboard, or plastic. Printed onto the support member **42** are the machine-readable data **36**, the first human-readable image **44**, and an indication **100** of a prepaid amount. The machine-readable data **36** includes a bar code which identifies the device **40**. The first human-readable image **44** includes a logo which identifies a transaction service.

Also printed onto the member **42** is a bar code **102** for linking the network access apparatus **32** to a resource provided by the computer **20** or the computer **64**. Preferably, the bar code **102** encodes an electronic address such as a URL (uniform resource locator) or an IP (Internet Protocol) address for a resource (such as a Web page) associated with either the computer **20** or the computer **64**. In general, the bar code **102** can include any of the machine-readable data for network navigation devices described in the above-listed patent application references which are incorporated by reference into this disclosure.

The prepaid transactions can be monitored in accordance with the teachings in the reference entitled "Methods and Systems for Providing a Resource in an Electronic Network", which is incorporated by reference into this disclosure.

FIG. **5** is a view of a first example of the device **52** described with reference to FIG. **1**. The member **53** of the device **52** includes a substantially flat substrate formed of a dielectric material such as paper, cardboard, or plastic. Printed onto the member **53** are the machine-readable data **50**, the first human-readable image **56**, and the second human-readable image **60**.

The second human-readable image **60** includes a graphical image **110** of the item itself and a price **112** associated with the item. The machine-readable data **50** includes a bar code for linking the network access apparatus **32** to a resource for purchasing the item. The first human-readable image **56** includes a logo identifying a transaction service to purchase the item. Since the logo corresponds to the logos illustrated in FIGS. **2** to **4**, the end user **26** recognizes that the examples of the device **40** described in FIGS. **2** to **4** can be used to purchase the item via the electronic network **22**.

The end user **26** can purchase the item by: (i) linking to a destination which provides the transaction service (e.g. by

reading the bar code **70** in FIG. **2** or the bar code **102** in FIG. **4** using the data reader **30**); (ii) reading the machine-readable data **50** using the data reader **30**; and (iii) reading the machine-readable data **36** from the device **40**. Alternatively, step (i) can be eliminated if the machine-readable data **50** initiates a link to the computer **20**. The network access apparatus **32** communicates the data via the electronic network **22** to facilitate the purchase.

FIG. **6** is a view of a second example of the device **52** described with reference to FIG. **1**. The member **54** of the device **52** includes either an item **120**, a housing **122** for the item **120**, packaging material for the item **120**, or a price sticker **124** associated with the item **120**. In this example, the item **120** is illustrated as a compact disk or a DVD. The compact disk or DVD can contain computer-readable data, audio data such as music, or video data such as a movie, for example. The housing **122** includes a jewel case for the compact disk or the DVD. It is noted, however, that other items and housings are contemplated for the device **52**.

The packaging material can include a wrapper or a package to contain the housing **122** and/or the item **120**. Alternatively, the packaging material can include a sheet of material, a booklet, an instruction manual associated with the item **120**. The price sticker **124** can be attached to either the item **120**, the housing **122**, or the packaging material.

The machine-readable data **50** supported by the member **54** includes a bar code which identifies the item **120**. Preferably, the bar code indicates the type of product or item being identified, a manufacturer of the item, and a product number associated with the item. As such, it is preferred that the bar code includes a UPC code, such as a UPC-A code or a UPC-E code, presently associated with most products. Optionally, the bar code can further include a code for a country of origin of the item. In this case, the bar code can include an EAN/JAN code such as an EAN/JAN-**8** code or an EAN/JAN-**13** code.

The end user **26** purchases the item **120** by: (i) linking to a destination which provides the transaction service (e.g. by reading the bar code **70** in FIG. **2** or the bar code **102** in FIG. **4** using the data reader **30**); (ii) reading the machine-readable data **50** using the data reader **30**; and (iii) reading the machine-readable data **36** from the device **40**. The network access apparatus **32** communicates the data via the electronic network **22** to facilitate the purchase of the item **120**.

FIG. **7** is a view of a third example of the device **52** described with reference to FIG. **1**. In this example, the device **52** includes a statement of charges, such an invoice or a bill, from a creditor.

The member **54** of the device **52** includes a substantially flat substrate formed of a dielectric material such as paper, cardboard, or plastic. Printed onto the member **54** are the machine-readable data **50**, the first human-readable image **56**, and the second human-readable image **60**.

The second human-readable image **60** includes an indication **130** of the creditor, an indication **132** of an amount due to the creditor, and an indication **133** of the debtor (such as the name of the end user **26**). The machine-readable data **50** includes a bar code for linking the network access apparatus **32** to a resource for paying the bill. The first human-readable image **56** includes a logo identifying a transaction service which can be used to pay the bill. Since the logo corresponds to the logos illustrated in FIGS. **2** to **4**, the end user **26** recognizes that the examples of the device **40** described in FIGS. **2** to **4** can be used to pay the bill via the electronic network **22**.

Using the data reader **30**, the end user **26** pays the bill by: (i) reading the machine-readable data **50** to link the network access apparatus **32** to a resource for paying the bill; (ii) reading a bar code **134** indicating a reference code for the bill; and (iii) reading the machine-readable data **36** from the device **40**. The network access apparatus **32** communicates the data via the electronic network **22** to facilitate the payment.

FIG. **8** is an illustration of an example of the data reader **30** and the network access apparatus **32** at the user location. In this example, the network access apparatus **32** comprises a personal computer **140**, and at least one input device including a keyboard **142** and a mouse **144**. The display device **34** comprises a monitor connected to a video port of the personal computer **140**. The data reader **30** includes a bar code reader connected to a serial port of the personal computer **140**.

The personal computer **140** includes a modem, a network adapter, or other transceiver for communicating with the electronic network **22**. The modem or the network adapter can communicate with the electronic network **22** via a line **146** such as a telephone line, an ISDN line, a coaxial line, a cable television line, a fiber optic line, a computer network line, or the like. Alternatively, the modem or the network adapter can wirelessly communicate with the electronic network **22**.

FIG. **9** is a flow chart summarizing steps performed in an embodiment of a transaction method. As indicated by block **160**, the method includes a step of receiving first data via the electronic network **22**. The first data indicates an item in a transaction.

As indicated by block **162**, the method includes a step of receiving second data via the electronic network **22**. The second data indicates a party of the transaction. The second data is read by an optical data reader in communication with the electronic network **22**.

As indicated by block **164**, the method includes a step of approving the transaction based upon the second data. The step of approving can be performed locally, or can be performed remotely by sending a first message based upon the second data and receiving a second message which authenticates the second data.

As indicated by block **166**, the method includes a step of creating a record of the transaction. Preferably, the record includes data representative of at least two of a date of the transaction, a time of the transaction, the party, the item, and a charged amount.

FIG. **10** is a flow chart summarizing steps performed in another embodiment of a transaction method. As indicated by block **170**, the method includes a step of receiving first data via the electronic network **22**. The first data indicates a first party in a transaction.

As indicated by block **172**, the method includes a step of receiving second data via the electronic network **22**. The second data indicates a second party of the transaction. The second data is read by an optical data reader in communication with the electronic network **22**.

As indicated by block **174**, the method includes a step of approving the transaction based upon the second data. The step of approving can be performed locally, or can be performed remotely by sending a first message based upon the second data and receiving a second message which authenticates the second data.

As indicated by block **176**, the method includes a step of sending a message indicating the transaction to the first

party. Preferably, the message includes data representative of at least two of a date of the transaction, a time of the transaction, a name associated with the second party, an address associated with the second party, an electronic address associated with the second party, the item, and a charged amount.

FIG. **11** is a flow chart summarizing steps performed in an embodiment of an authentication method in accordance with the present invention.

As indicated by block **180**, the method includes a step of receiving data associated with a time-varying bar code. The data can be received via the electronic network **22** or another network by the computer **64**. Preferably, the data is read by a bar code reader at the user location **24**.

As indicated by block **182**, the method includes a step of approving a transaction based upon the data. The transaction is approved or disapproved based upon a step of comparing the data to data generated by a code generator synchronized to the time-varying bar code.

Thus, there has been described herein several embodiments including preferred embodiments of transaction methods, systems, and devices.

Because the various embodiments of the present invention authenticate an end user in a transaction based upon machine-readable data read by a data reader at the end user's location, they provide a significant improvement in that the end user does not have to recall a personal identification number to perform the transaction.

Additionally, the various embodiments of the present invention authenticate an end user using a time-varying bar code to foil unauthorized transactions using a fixed personal identification code.

It will be apparent to those skilled in the art that the disclosed invention may be modified in numerous ways and may assume many embodiments other than the preferred form specifically set out and described above.

Accordingly, it is intended by the appended claims to cover all modifications of the invention which fall within the true spirit and scope of the invention.

What is claimed is:

1. A transaction method comprising the steps of:

providing a computer accessible via an electronic network at an electronic address encoded by a bar code supported by a member;

receiving a first data element by the computer and via the electronic network, the first data element read by a bar code reader in communication with the electronic network, the first data element indicating a first party of a transaction;

receiving a second data element by the computer and via the electronic network, the second data element read from the member by the bar code reader in communication with the electronic network, the second data element indicating a second party of the transaction;

authenticating the second data element; and upon authenticating the second data element, sending a message based on the transaction to the first party.

2. The transaction method of claim **1** wherein the message includes data representative of at least two of a date of the transaction, a time of the transaction, a name associated with the second party, an address associated with the second party, an electronic address associated with the second party, the item, and a charged amount.

3. A transaction system comprising:

a computer in communication with an electronic network to receive a first data element and a second data element both read by a bar code reader, the first data element indicating a first party of a transaction, the second data element indicating a second party of the transaction;

wherein the computer authenticates the second data element and sends a message indicating the transaction to the first party upon authenticating the second data element; and

wherein the computer is accessible via the electronic network at an electronic address encoded by a bar code supported by a member having the second data element.

4. The transaction system of claim **3** wherein the message includes data representative of at least two of a date of the transaction, a time of the transaction, a name associated with the second party, an address associated with the second party, an electronic address associated with the second party, the item, and a charged amount.

5. A transaction device comprising:

a member;

a first bar code supported by the member, the first bar code providing an instruction for linking to a destination in an electronic network; and

a second bar code supported by the member, the second bar code providing an identification code for authenticating a transaction at the destination.

6. The transaction device of claim **5** wherein the first bar code encodes an electronic address for the destination.

7. The transaction device of claim **6** wherein the electronic address includes at least a portion of a uniform resource locator.

8. The transaction device of claim **5** further comprising a human-readable image supported by the member, the human-readable image associated with the destination.

9. The transaction device of claim **5** wherein the member is credit-card-shaped.

10. The transaction device of claim **5** further comprising a display device supported by the member, the display device to display the second bar code.

11. A transaction device comprising:

a member selected from the group consisting of a credit card, a debit card, an automatic teller machine card, and a charge card;

a first bar code supported by the member, the first bar code encoding an electronic address of a destination in an electronic network; and

a second bar code supported by the member, the second bar code providing an identification code for authenticating a transaction at the destination.

12. The transaction device of claim **11** further comprising a display device supported by the member, the display device to display the second bar code.

13. A method of facilitating a transaction between a first party and a second party, the method comprising the steps of:

providing a computer accessible via an electronic network;

providing a first member which supports a first bar code, a second bar code and a human-readable image, the first bar code encoding an electronic address for linking to the computer, the second bar code encoding an identification code for the second party, the human-readable image including a transaction service logo;

receiving, via the electronic network, a link to the computer based upon the first bar code;

receiving, by the computer and via the electronic network, the identification code read from the second bar code;

receiving, by the computer and via the electronic network, data read from a third bar code supported by a second member, the data indicating both an item in the transaction and the first party, the second member having a human-readable image which includes the transaction service logo;

approving the transaction based upon the identification code for the second party; and

sending a message indicating the transaction to the first party.

14. The method of claim **13** wherein the third bar code is selected from the group consisting of a UPC code and an EAN/JAN code.

15. The method of claim **13** wherein the message includes data representative of a date of the transaction, a time of the transaction, a name associated with the second party, the item, and a charged amount.

16. The method of claim **13** wherein the second member supports a human-readable image of the item.

17. The method of claim **13** wherein the electronic network comprises an internet.

18. The method of claim **13** wherein the electronic network comprises an intranet.

19. A method of facilitating a transaction between a first party and a second party, the method comprising the steps of:

providing a computer accessible via an electronic network;

providing a first member which supports a first bar code and a second bar code, the first bar code encoding an electronic address for linking to the computer, the second bar code encoding an item in the transaction;

receiving, via the electronic network, a link to the computer based upon the first bar code;

receiving, by the computer and via the electronic network, a data element indicating the item in the transaction from the second bar code;

receiving, by the computer and via the electronic network, a data element read from a third bar code supported by a second member, the third bar code encoding an identification code for the second party; and

processing the transaction based upon at least the identification code.

20. The method of claim **19** wherein the first member supports a human-readable image including a transaction service logo, and wherein the second member supports a human-readable image including the transaction service logo.

21. The method of claim **19** wherein the first member comprises a printed invoice.

22. The method of claim **19** wherein the electronic network comprises an internet.

23. The method of claim **19** wherein the electronic network comprises an intranet.

* * * * *

US005956699A

United States Patent [19]

Wong et al.

[11] Patent Number: 5,956,699

[45] Date of Patent: Sep. 21, 1999

[54] **SYSTEM FOR SECURED CREDIT CARD TRANSACTIONS ON THE INTERNET**

[75] Inventors: **Jacob Y. Wong**, Goleta; **Roy L. Anderson**, Glendale, both of Calif.

[73] Assignee: **Jaesent Inc.**, Goleta, Calif.

[21] Appl. No.: **08/971,272**

[22] Filed: **Nov. 17, 1997**

Related U.S. Application Data

[63] Continuation-in-part of application No. 08/720,785, Oct. 3, 1996.

[51] **Int. Cl.**[6] **G06F 17/60**

[52] **U.S. Cl.** **705/39**; 235/380; 340/825.33; 380/23; 380/24; 380/42; 380/43; 705/26; 705/44

[58] **Field of Search** 705/35, 26, 27, 705/38, 39, 40, 41, 42, 43, 44; 340/825.3, 825.31, 825.33, 825.34; 235/375, 380, 379, 382, 382.5; 380/23, 24, 25, 42, 43, 4; 902/2, 4, 5

[56] **References Cited**

U.S. PATENT DOCUMENTS

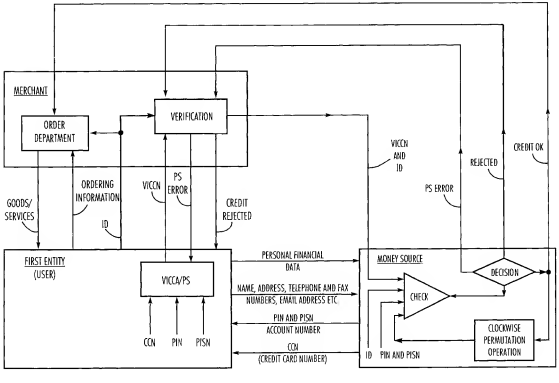
5,557,518 9/1996 Rosen 380/24
5,671,280 9/1997 Rosen 380/24

Primary Examiner—Stephen R. Tkacs
Attorney, Agent, or Firm—Lyon & Lyon LLP

[57] **ABSTRACT**

A method for providing secure credit card transactions over the Internet generates a personal charge number from a user account number by inserting a user key into the user account number in accordance with an algorithm that uses a user insertion key and a permutation variable. After the personal charge number is used, the permutation variable is changed, and a new personal charge number is generated. A money source repository verifies the validity of the personal charge number by using the personal charge number and a user identifier to access a file with the user account number, the user key and the user insertion key, taking into account which permutation variable is valid at a given point in time. Alternatively, the money source repository could generate a string of valid personal charge numbers for a user which are sequentially accessed according to usage.

18 Claims, 1 Drawing Sheet



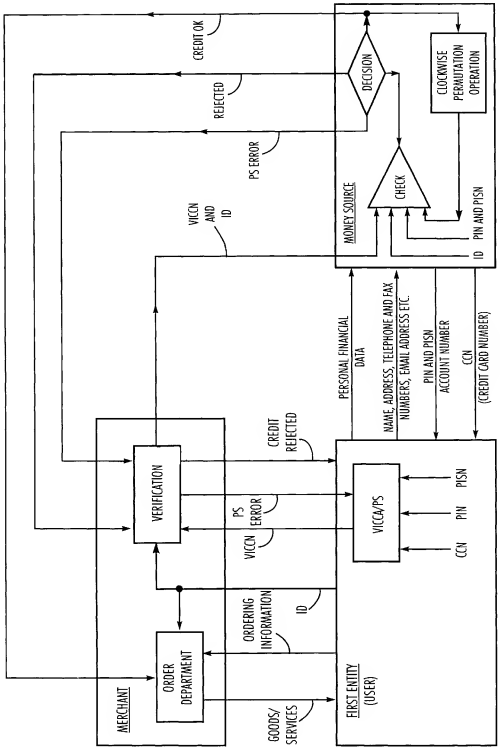

MERCHANT
ORDER DEPARTMENT
VERIFICATION
VICCA/PS
FIRST ENTITY (USER)
MONEY SOURCE
DECISION
CHECK
CLOCKWISE PERMUTATION OPERATION
CREDIT OK
REJECTED
PS ERROR
VICCN AND ID
ORDERING INFORMATION
ID
GOODS/ SERVICES
PS ERROR
VICCN
CREDIT REJECTED
CCN
PIN
PISN
PERSONAL FINANCIAL DATA
NAME, ADDRESS, TELEPHONE AND FAX NUMBERS, EMAIL ADDRESS ETC.
PIN AND PISN
ACCOUNT NUMBER
CCN
(CREDIT CARD NUMBER)
ID
PIN AND PISN

Fig. 1

SYSTEM FOR SECURED CREDIT CARD TRANSACTIONS ON THE INTERNET

CROSS-REFERENCE TO RELATED APPLICATIONS

This present application is a continuation-in-part of U.S. application Ser. No. 08/720,785 filed on Oct. 3, 1996 for SYSTEM AND METHOD FOR PSEUDO CASH TRANSACTIONS. The disclosure of that application is specifically incorporated herein by reference.

FIELD OF THE INVENTION

The present invention is in the field of electronic money/Internet payment systems.

BACKGROUND OF THE INVENTION

As the Internet continues to transform commerce as we know it, method of payment is one component that is critical to successfully conducting business across a network. Today shoppers purchasing goods or services on the Internet are required to give their credit card numbers, phone numbers and/or addresses over the Internet in order to complete their transactions. The problem is that they do not know who else might be able to retrieve this information without their knowledge or consent. No doubt people are still very enthusiastic about the idea of Internet commerce. However, they are much more reserved in believing its potential, all because of the issues of privacy and potential credit liability not being fully resolved and protected in shopping on the internet at the present time.

U.S. application Ser. No. 08/720,785 filed on Oct. 3, 1996 for SYSTEM AND METHOD FOR PSEUDO CASH TRANSACTIONS cited and reviewed five electronic payment systems for use on the Internet, viz. First Virtual, Cybercash, Netbill, Millicent and Digicash or ecash. The conclusion was that no satisfactory systems and/or procedures for electronic money/Internet payment existed. However, since personal privacy and credit liability will no doubt continue to be issues of great importance for potential Internet users, commerce on the Internet simply cannot flourish without a cash dispensing system that not only guarantees these features, but also others that take advantage of the simplicity and convenience of buying and selling on the Internet.

In order to fill such an urgent need, a novel system and method for pseudo cash transactions was advanced in U.S. application Ser. No. 08/720,785 Through this system, totally anonymous or effectively anonymous cash-like transactions are accomplished by using a pseudo cash data packet converter for inserting a user key into a pseudo cash preliminary data packet through the use of a user insertion key to generate a pseudo cash unit with a fixed monetary value that can be used to purchase goods or services via the Internet. A pseudo cash repository facilitates the cash the cash-like transactions and maintains a record of the pseudo cash units and their fixed monetary value. Depending upon the level of anonymity selected by a purchaser, the pseudo cash repository can either transmit pseudo cash preliminary data packets or pseudo cash units to a first entity. If the first entity loses an effectively anonymous pseudo cash preliminary data packet, it can be replaced by the pseudo cash repository.

Since the filing date of the aforementioned U.S. application Ser. No., 08/720,785, viz. Oct. 3, 1996, additional electronic payment systems for the Internet have been

advanced (see for example, *Electronic Payment Systems,* by Donald O'Mahoney et al., ISBN: 0-89006-925-5, and published by ARTECH HOUSE PUBLISHERS, 1997). Not necessary in chronological order or in completeness, some of these important systems are listed and reviewed as follows.

Magic Money is a system proposed for the implementation of fully anonymous digital cash using blind signatures. It has many similarities with the Digicash or Ecash system cited earlier in the application Ser. No. 08/720,785, and was designed for experimental purposes by a group of cryptographic enthusiasts, know as cypherpunks, on the Internet. The source code is available in computer software language C and there is an example client program that can automatically accept and pay out Magic Money currency. This system is set up purposely to be rather complex and the users are required to have extensive knowledge in computer software before they can use the system efficiently.

Project CAFÉ is an advanced electronic payment system developed as the result of a project funded by the European Community and started in 1992. CAFÉ is a hybrid scheme in the sense that it offers all the benefits of anonymous electronic cash but at the same time lets the user sign checks up to a specified amount. It is an advanced payment mechanism that makes use of secure tamper-resistant devices such as smart cards and strong cryptographic protocols. It also provides untraceable electronic payments and guarantees the security of all parties concerned. However, this advanced electronic payment system is necessarily a very complex system involving the cooperation and participation of many willing players and hence not especially efficient and simple for use in the Internet by the general public.

NetCash is an identified online electronic cash system, for open networks. It consists of distributed currency users that mint electronic coins and issue them to the users of the system, accepting electronic checks in payment for them. The system is online in that each coin must be verified as being valid and unspent by forwarding it to the minting currency server for verification during a purchase. Although the digital cash is identified, with each coin having a unique serial number, there is an exchange mechanism to provide limited anonymity. Anyone with valid coins can exchange them anonymously with a currency server for new ones.

NetCash is a macropayment system suitable for selling hard goods, information, or other network services. Users can both make and accept payments. It is a software-only solution, requiring no special hardware. Both asymmetric and symmetric cryptography is used to provide the network security of the system and to limit fraud. Unfortunately, like the previously cited electronic cash payment systems, it encompasses too many facets of application and is certainly more complex than is needed for doing simple commerce electronic transactions on the Internet.

Both Mondex and EMV Cash Card are electronic cash card or prepayment card systems to effect payment in the retail context. Their scheme involves preloading a chip card with value that could then be spent at retail outlets. As such, this electronic cash systems, without a major structural redesign, is not suitable for use with the Internet.

Besides electronic cash payment systems alluded to above, there are also credit card-based systems such as MOTO (Mail order/telephone order transactions). Unsecured network payments, First Virtual (cited earlier in application Ser. No. 08/720,785), CARI (Collect all relevant information), SSL (secure socket layer) and SET (Secure Electronic Transactions). All of these credit card-based

payment systems use sophisticated software packages, secure tamper-resistant hardware devices and strong cryptographic protocols involving the users, the merchants and the issuing money sources.

There are two fundamental characteristics that are common to all electronic card payment and credit card-based payment systems today. First, security and privacy of vital personal information that is transmitted over the Internet are always entrusted by the user to the money source such as the bank, credit card company etc. In other words, the user gives out the vital personal information directly on the Internet and relies solely on embedded software at his or her computer (supplied in many cases by the money source) or the server of the money source for encryption of such information before it appears publicly on the Internet. Thus it depends on how secured the individual user feels before he or she is willing to give out their vital personal information, irrespective of what electronic cash or credit card-based systems that he or she uses. Sometimes even an iron-clad guarantee by these electronic cash or credit card-based system sponsors may not be good enough to influence an individual user's decision to conduct or not to conduct commerce on the Internet using either some form of digital cash or credit cards. In fact, as alluded to earlier, until such time that a simple electronic cash system, trusted absolutely 100% by the users on the Internet, becomes available, security of privacy remains as the single most important issue that will stymie the future growth of commerce on the Internet.

Second, transactions on the Internet for practically all electronic cash or credit-card-based systems of today invariably involve a three-way interaction, namely among the user, the merchant and the money source. This characteristic or feature of present day systems not only requires the system structure to be necessarily more complex, it also generally takes more time and is more costly for transactions to take place on the Internet.

The novel system for processing electronic cash transactions anonymously (or code-named SPECTA) on the Internet, as advanced in U.S. application Ser. No. 08/720,785 filed on Oct. 3, 1996, significantly reduces the role of merchants in any Internet commerce transaction to just verifying the validity of the digital cash tendered or the user's credit card (to be discussed below). It also simplifies any transaction on the Internet from a three-party interaction to that of only two. Furthermore, the SPECTA system allows the user to encrypt very simply his or her vital personal information (such as digital cash, name and address, telephone or credit card numbers etc.) himself or herself, before placing such information on the Internet. This feature might appear to be routine and superficial on the surface. However, from the security standpoint, it is extremely important. The reason is that by having the user encrypt just his or her own vital information on the Internet, it eliminates the desire for any pirate to decode such information. Contrary to cracking the encryption code of a money source, which could lead to a wealth of vital information that possesses monetary value, there is simply not enough monetary inventive to crack just one or two individual users' encryption codes on the Internet. Thus the SPECTA system by design offers a much stronger security to safeguard the privacy of personal information for users on the Internet.

It is an object of the present invention to extend the SPECTA electronic cash transaction system, which was filed as U.S. application Ser. No. 08/720,785 on Oct. 3, 1996 for SYSTEM AND METHOD FOR PSEUDO CASH TRANSACTIONS, to include the use of credit cards for conducting commerce on the Internet. This feature is especially important as more and more Internet users gain confidence to do commerce on the Internet and prefer to use the more convenient credit cards to pay for goods and services tendered to them.

SUMMARY OF THE INVENTION

The present invention is generally directed to electronic money/Internet payment systems that insert a user key into a user account number in accordance with a user insertion key through use of an algorithm to generate a personal charge number so customers and vendors can buy and sell merchandise and information on the Internet in a manner resembling real-life credit card transactions.

In a first, separate aspect of the present invention, a permutation variable is used to generate different personal charge numbers from a user account number according to a valid state of the permutation variable. A user transfers the personal charge number and a user identifier, such as a name or social security number, to a vendor. The vendor can then transmit the personal charge number and user identifier, along with a transaction monetary value, to a money source repository for payment. If the personal charge number is validated for the user, the vendor is paid and the user is charged for the transaction. Once a personal charge number is used, the permutation variable is changed, and the personal charge number will no longer be valid.

In another, separate aspect of the present invention, the permutation variable is a permutation state of the user insertion key. The permutation state can be varied by simple clockwise rotation. Using this variation, a personal charge number will cycle through periods of being valid or invalid according to a very simple selection process.

In yet another, separate aspect of the present invention, a list of valid personal charge numbers for a user is generated by a Money Source. As the user uses a valid personal charge number, it is deactivated and the next personal charge number is activated. In this manner, the Money Source can scroll through a list of valid personal charge numbers for a user. If any of the inputs used to create the list are varied, the list can be replaced by a newly generated list.

Accordingly, it is a primary object of the present invention to provide an improved payment system suitable for use on the Internet, which allows buyers and sellers to conduct credit card transactions.

This and further objects and advantages will be apparent to those skilled in the art in connection with the drawings and the detailed description of the preferred embodiments set forth below.

BRIEF DESCRIPTION OF THE DRAWING

FIG. 1 is a schematic drawing depicting a system and method for conducting commerce on the Internet with a credit card according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is an extension of the SPECTA system disclosed in U.S. application Ser. No. 08/720,785 filed on Oct. 3, 1996 as referred to earlier. The SPECTA system enables pseudo cash transactions to be conducted on the Internet by relying upon pseudo cash units generated by insertion of user keys into pseudo cash preliminary data packets in accordance with user insertion keys through the use of an algorithm. In a similar way, the present invention

enables credit transactions to be conducted on the Internet by relying upon convenient and secured valid Internet credit card numbers (VICCN) generated by insertion of user keys into user account numbers in accordance with user insertion keys through the use of a slightly more complicated algorithm which uses permutation variables.

A preferred embodiment of the present invention, which uses VICCN generated by a Money Source, is depicted in FIG. 1. A first entity (user) must initially establish a business relationship with the Money Source which assigns the first entity a user account number and enters into an agreement with the first entity regarding use of the account number. The user account number can represent an actual account number that the first entity has with the Money Source, such as a credit card number, a savings account number, a checking account number, a money market number, a brokerage account number, etc., or it can simply be an identification number assigned to the first entity by the Money Source. Although the preferred embodiment is hereinafter described in connection with credit card or charge transactions, the invention is equally applicable to other financial transactions involving debits and credits, such as checking transactions or direct withdrawals from an existing account. Once the first entity establishes an account number with the Money Source, the first entity selects (or the Money Source assigns to the first entity) a Personal ID Number or PIN and a PIN Insertion Sequence Number (PISN) and a record associated with the first entity is generated by the Money Source in a money source repository. The record will include the user account number of the first entity, the user key of the first entity, the user insertion key of the first entity and a first entity identifier (ID). The ID can take the form of any number of buyer identification information, such as name, shipping address, email address, phone or fax number, social security number, buyer identification number, etc. It is contemplated that the record will be maintained electronically in a secure data base by the Money Source, and the exact form and parameters of the record, as well as its generation and maintenance, should be well within the skill of one of ordinary skill in the art of computer programming. Further, the term "record" could encompass multiple data files, so long as the referenced information is stored somewhere such that it can be retrieved or linked together as necessary to carry out the requisite functions of the present invention.

The novel methodology advanced in the present invention is to allow the user to encrypt the user's personal charge number (CCN) in a very simple fashion according to the SPECTA system and include the additional important feature of the PISN Permutation State in the generation of a VICCN for use in commerce on the Internet. When the personal charge number is used for the first time on the Internet, the Permutation State (PS) of the PISN, or PSNPS, is simply the original PISN as first assigned to or selected by the first entity. For example, suppose the user's CCN is "1234567891234567", the PIN is "7890" and the PISN is "2468". Then the VICCN, when the credit card is used for the first time on the Internet, is (for PISNPS=2468) simply "1(7)2(8)3(9)4(0)56789123456". When the personal charge number is used the second time, the PISNPS must be changed by a simple clockwise rotation permutation in which the new PISNPS becomes "4682" or the effective PISN=4682. The new VICCN, when the personal charge number is used the second time, is now "1(0)2(7)3(8)4(9)56789123456". For the four digit PISN of 2468, there are a total of four available PISNPS states through use of a simple clockwise rotation permutation: "2468", "4682", "6824" and "8246". Thus the VICCN for use in Internet commerce is different for each different PISNPS dependent upon which state is prevalent at the time of using the personal charge number on the Internet.

At the request of the first entity, the Money Source could also make available to the first entity a device called Valid Internet Credit Card Arranger (VICCA) which helps the first entity in generating the Valid Internet Credit Card Number (VICCN) for use on the Internet according to the present invention. The VICCA takes as inputs the first entity or user's PIN, PISN and CCN, and then combines this information to generate a Valid Internet Credit Card Number (VICCN), taking into consideration automatically the so-called PISNPS Permutation State. The Permutation State of the PISN is defined as the N possible clockwise permutation allowed when N is the number of numerical (or alphanumerical) digits contained in the PISN. Thus, for example, N=4 if PISN =2468. Then the number of possible permutation state is four as alluded to earlier.

When the first entity's personal charge number is used for the first time, the initial PISN defines the fist Permutation State or PISNPS. The VICCA automatically takes into consideration the PISNPS needed to generate the VICCN, every time the personal charge number is used on the Internet, by performing the necessary clockwise rotation permutation of the PISN after every use of the personal charge number. The VICCA is meant only as a convenience device for the first entity who can also keep track of the Permutation State without use of the VICCA to arrive at the same VICCN every time the personal charge number is used for commerce on the Internet.

Thus, for the first entity to conduct commerce on the Internet, the first entity first sends the order information, the first entity's ID and a VICCN to the merchant through the Internet. The merchant in turn sends the ID and VICCN along with a transaction monetary value via the Internet to the Money Source for verification. Knowing the user ID and the VICCN, the Money Source can quickly verify that the VICCN is valid for the first entity, verify that the transaction monetary value is within the limits of transactions available to the first entity through use of the user account number that was used to generate the VICCN, and then send the merchant a confirmation or verification of the validity of the transaction on the Internet. Thereafter, the merchant could be paid, and the first entity could be billed, in the same fashion that credit card companies currently handle credit card transactions. Moreover, the Money Source could charge the merchant and/or the first entity a portion of the transaction monetary value as a fee for providing such services.

An advantage of the preferred embodiment is that it can easily be adopted for use in existing systems with a minimum of difficulty and without the need for complicated training of users. If the Money Source is a company that already issues credit cards, existing credit card numbers could be used for the personal charge numbers of users of the system. In such a situation, the present invention enables the first entity to conveniently conduct commerce on the Internet without fear of security break on the first entity's personal ID or financial liability because the existing credit card number is not transmitted naked on the Internet. Instead, the existing credit card number is encrypted and converted into a VICCN. Thus, to obtain the credit card number of the first entity from use of the VICCN on the Internet, a pirate would have to decrypt the VICCN. Furthermore, if the VICCN is intercepted and used, it will not be valid unless the permutation variable used to generate the VICCN is valid at the time that a person pirating the VICCN tries to use the VICCN.

In an alternative embodiment, instead of creating a record of information used to generate a VICCN for a first entity with the Money Source, the Money Source could use such information to generate a "record" of valid VICCN for the first entity, depending upon the correct state of the permutation variable. In this embodiment, after a vendor transmits

a VICCN and first entity identifier to the Money Source, the Money Source would verify that the VICCN is in fact valid. Once validity is confirmed and the transaction is processed, the VICCN would no longer be valid and a new VICCN would be needed for a valid transaction from the first entity. In its simplest form, the Money Source could simply create a string of personal charge numbers associated with the first entity that are accessed by a rolling scroll mechanism. Further, to the extent that any of the variables used to create the string are subsequently varied, the list could simply be regenerated.

The above discussion of this invention is directed primarily to the preferred embodiments and practices thereof. Further modifications are also possible in alternative embodiments without departing from the inventive concept. Thus, for example, methods other than clockwise rotation could be used to alter the permutation variable. For example, a number could be added to one of the digits of the PIN or the PISN in a sequential fashion or one of digits could be sequentially varied.

Accordingly, it will be readily apparent to those skilled in the art that still further changes and modifications in the actual concepts described herein can readily be made without departing from the spirit and scope of the invention as defined by the following claims.

What is claimed:

1. A method for providing secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) assigning a user account number to the first entity;

(2) generating a record associated with the first entity with a money source repository which includes the user account number of the first entity, a user key, a user insertion key and a first entity identifier;

(3) generating a personal charge number from the user account number by inserting the user key into the user account number in accordance with an algorithm that uses the user insertion key and a permutation variable;

(4) transferring the personal charge number and the first entity identifier to a second entity;

(5) transmitting the personal charge number, the first entity identifier, a transaction monetary value and a second entity identifier from the second entity to the money source;

(6) verifying that the personal charge number is valid for the first entity;

(7) providing the second entity with a monetary credit associated with the transaction monetary value; and

(8) charging the first entity with a charged credit associated with the transaction monetary value.

2. A method as recited in claim **1**, wherein the monetary credit is equal to or less than the transaction monetary value.

3. A method as recited in claim **2**, wherein the charged credit is equal to or greater than the monetary credit.

4. A method as recited in claim **1**, comprising the additional steps of:

(9) changing the permutation variable from an initial state to a different state; and

(10) repeating steps (3) through (8).

5. A method as recited in claim **4**, wherein the permutation variable is a permutation state of the user insertion key.

6. A method as recited in claim **5**, wherein the permutation state of the user insertion key is changed by rotation.

7. A method as recited in claim **4**, wherein the personal charge number generated in step (3) is different from the personal charge number that is generated when step (3) is repeated.

8. A method as recited in claim **7**, comprising the additional steps of:

(11) repeating steps (9) and (10).

9. A method as recited in claim **8**, wherein the personal charge number generated as part of step (11) is different from the personal charge number that is generated as part of step (10) or as part of step (3) before it is repeated as part of step (10).

10. A method as recited in claim **4**, wherein the permutation variable is an additional digit added to the user insertion key.

11. A method as recited in claim **4**, wherein the permutation variable is an additional digit added to the user key.

12. A method as recited in claim **1**, wherein the personal charge number will not be verified as valid in step (6) unless the permutation variable used to generate the personal charge number is valid at the time verification.

13. A method for providing secure transactions between a first entity and at least one additional entity, comprising the steps of:

(1) creating a record of a plurality of personal charge numbers for a first entity with a first entity identifier in a money source repository from a user account number of the first entity, a user key and a user insertion key by inserting the user key into the user account number in accordance with an algorithm that uses the user insertion key and a permutation variable which is varied to create each of the plurality of personal charge numbers;

(2) selecting a first of the plurality of personal charge numbers as being valid within the record to create a valid personal charge number associated with the first entity identifier;

(3) transferring the valid personal charge number and the first entity identifier to a second entity;

(4) transmitting the valid personal charge number, the first entity identifier, and a transaction monetary value from the second entity to the money source repository;

(5) verifying that the valid personal charge number is valid for the first entity;

(6) changing the first of the plurality of personal charge numbers to an invalid state and creating a new valid personal charge number from one of the remaining plurality of personal charge numbers;

(7) providing the second entity with a monetary credit associated with the transaction monetary value; and

(8) charging the first entity with a charged credit associated with the transaction monetary value.

14. A method as recited in claim **13**, wherein the monetary credit is equal to or less than the transaction monetary value.

15. A method as recited in claim **13**, wherein the charged credit is equal to or greater than the monetary credit.

16. A method as recited in claim **13**, comprising the additional steps of:

(9) repeating steps (3) through (8) until all of the plurality of personal charge numbers have been a valid personal charge number and then repeating the sequential process selection of valid personal charge numbers.

17. A method as recited in claim **13**, wherein the permutation variable is a permutation state of the user insertion key.

18. A method as recited in claim **17**, wherein the permutation state of the user insertion key is changed by rotation.

* * * * *

US006055573A

United States Patent [19]

Gardenswartz et al.

[11] Patent Number: 6,055,573

[45] Date of Patent: Apr. 25, 2000

[54] **COMMUNICATING WITH A COMPUTER BASED ON AN UPDATED PURCHASE BEHAVIOR CLASSIFICATION OF A PARTICULAR CONSUMER**

[75] Inventors: **Will H. Gardenswartz**, Annapolis, Md.; **David W. Banker**, Mt. Baldy, Calif.; **Melissa B. Goidel**, New York, N.Y.

[73] Assignee: **SuperMarkets Online, Inc.**, Greenwich, Conn.

[21] Appl. No.: **09/226,174**

[22] Filed: **Jan. 7, 1999**

Related U.S. Application Data

[60] Provisional application No. 60/114,462, Dec. 30, 1998.

[51] **Int. Cl.**[7] **G06F 13/00**

[52] **U.S. Cl.** **709/224**; 709/219; 709/223; 705/26

[58] **Field of Search** 709/201, 202, 709/206, 217, 218, 219, 223, 224; 705/26, 27, 10, 1; 707/10

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,882,675	11/1989	Nichtberger et al. .	
5,056,019	10/1991	Schultz et al. .	
5,201,010	4/1993	Deaton et al. .	
5,237,620	8/1993	Deaton et al. .	
5,249,044	9/1993	Von Kohorn .	
5,283,731	2/1994	Lalonde et al. .	
5,285,278	2/1994	Holman .	
5,287,181	2/1994	Holman .	
5,305,196	4/1994	Deaton et al. .	
5,353,218	10/1994	De Lapa et al. .	
5,380,991	1/1995	Valencia et al. .	
5,459,306	10/1995	Stein et al. .	
5,483,049	1/1996	Schulze, Jr. .	
5,592,560	1/1997	Deaton et al. .	
5,621,812	4/1997	Deaton et al. .	
5,636,346	6/1997	Saxe	705/1

(List continued on next page.)

FOREIGN PATENT DOCUMENTS

0 512 509 A2	11/1992	European Pat. Off. .
0 822 535 A2	2/1998	European Pat. Off. .
196 41 092 A1	4/1998	Germany .
WO 97/12486	4/1997	WIPO .
WO 97/23838	7/1997	WIPO .
WO 98/15907	4/1998	WIPO .

OTHER PUBLICATIONS

IntelliQuest Looks for Interaction with Loyalty, Web Traffic Programs, Electronic Advertising & Marketplace Report, Lexis–Nexis, Oct. 20, 1998.

IntelliQuest and CoolSavings Offer Innovative Online Customer Relationship Management Program for Technology Vendors, Business Editors & Technology Writers, Lexis–Nexis, Sep. 30, 1998.

In this Computer Age, Who Needs Coupons?, The New York Times, Jun. 15, 1989[1].

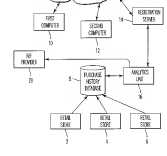
Primary Examiner—Viet D. Vu

Attorney, Agent, or Firm—Oblon, Spivak, McClelland, Maier & Neustadt, P.C.

[57] **ABSTRACT**

A method, system, and computer program product for delivering a targeted advertisement. A first identifier, such as a cookie, corresponding to the a first computer is received from the first computer. A targeted advertisement is delivered to the first computer in response to receiving the first identifier from the first computer. The targeted advertisement is based on the observed offline purchase history of a consumer associated with the first identifier. The invention includes the delivery of a promotional incentive for a consumer to comply with a particular behavioral pattern. The behavioral pattern may be a predefined change in purchase behavior or continuance of an established purchase behavior. The targeted advertisements sent to consumers may be changed and/or refined based on changes in consumers' purchase history behaviors.

12 Claims, 11 Drawing Sheets



U.S. PATENT DOCUMENTS

5,642,485	6/1997	Deaton et al. .	
5,644,723	7/1997	Deaton et al. .	
5,649,114	7/1997	Deaton et al. .	
5,687,322	11/1997	Deaton et al. .	
5,724,521	3/1998	Dedrick	705/26
5,761,648	6/1998	Golden et al. .	
5,806,044	9/1998	Powell .	
5,809,242	9/1998	Shaw et al.	709/217
5,809,481	9/1998	Baron et al.	705/14
5,832,457	11/1998	O'Brien et al. .	
5,845,396	12/1998	Gerace .	
5,852,775	12/1998	Hidary	455/404
5,855,007	12/1998	Jovicic et al. .	
5,855,008	12/1998	Goldhaber et al. .	
5,857,175	1/1999	Day et al. .	

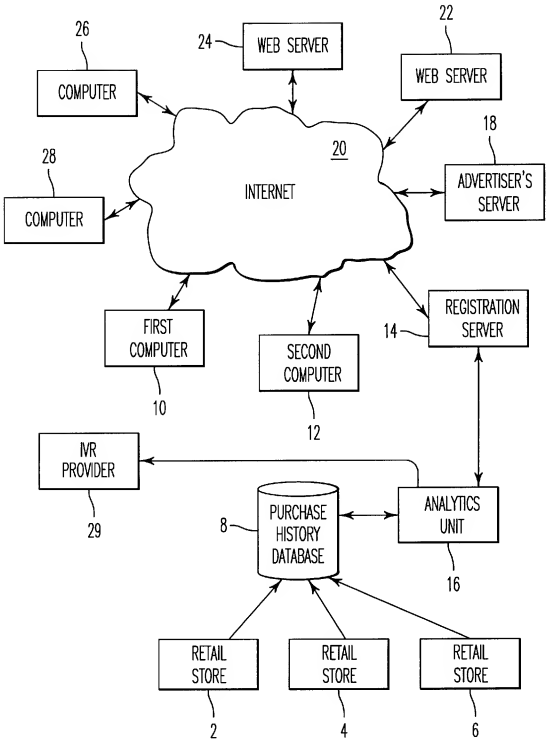

26
COMPUTER
24
WEB SERVER
22
WEB SERVER
18
ADVERTISER'S SERVER
20
INTERNET
28
COMPUTER
FIRST COMPUTER
10
SECOND COMPUTER
12
14
REGISTRATION SERVER
IVR PROVIDER
29
8
PURCHASE HISTORY DATABASE
ANALYTICS UNIT
16
RETAIL STORE
2
RETAIL STORE
4
RETAIL STORE
6

FIG. 1

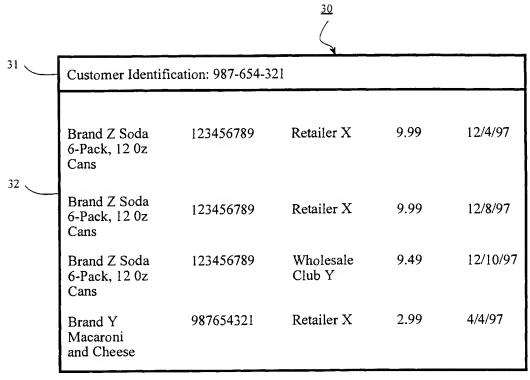


Figure 2(a)

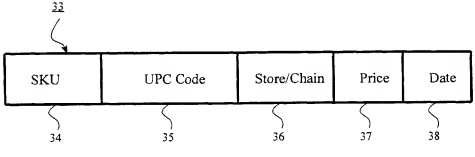


Figure 2(b)

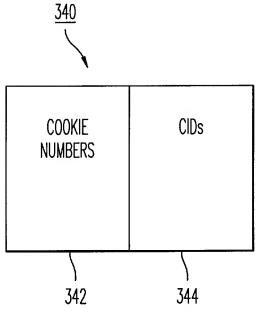


FIG. 3

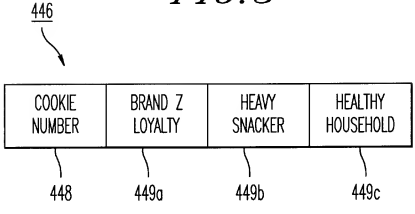


FIG. 4(a)

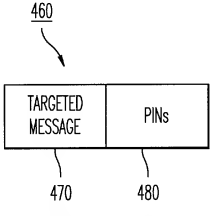


FIG. 4(b)

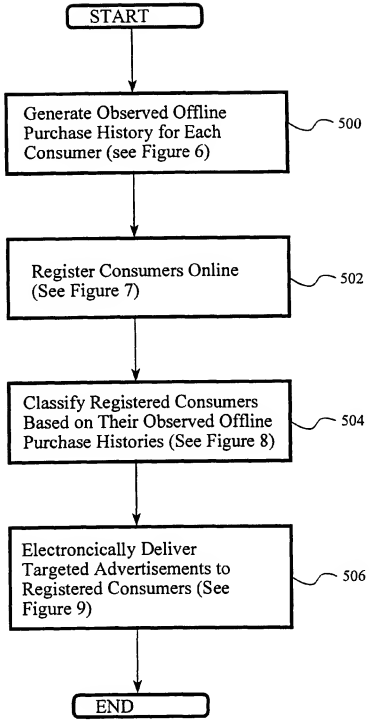

START
Generate Observed Offline Purchase History for Each Consumer (see Figure 6)
500
Register Consumers Online (See Figure 7)
502
Classify Registered Consumers Based on Their Observed Offline Purchase Histories (See Figure 8)
504
Electroncically Deliver Targeted Advertisements to Registered Consumers (See Figure 9)
506
END

Figure 5

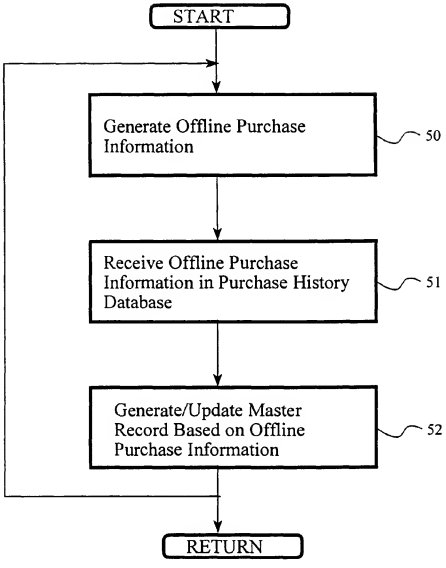

START
Generate Offline Purchase Information
50
Receive Offline Purchase Information in Purchase History Database
51
Generate/Update Master Record Based on Offline Purchase Information
52
RETURN

Figure 6

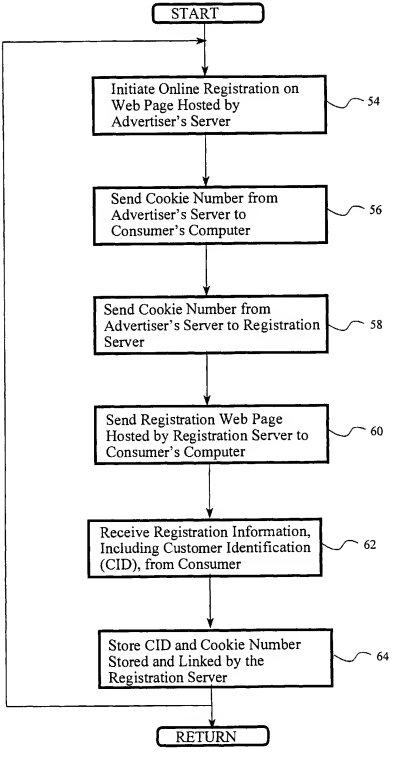

START
Initiate Online Registration on Web Page Hosted by Advertiser's Server
54
Send Cookie Number from Advertiser's Server to Consumer's Computer
56
Send Cookie Number from Advertiser's Server to Registration Server
58
Send Registration Web Page Hosted by Registration Server to Consumer's Computer
60
Receive Registration Information, Including Customer Identification (CID), from Consumer
62
Store CID and Cookie Number Stored and Linked by the Registration Server
64
RETURN

Figure 7

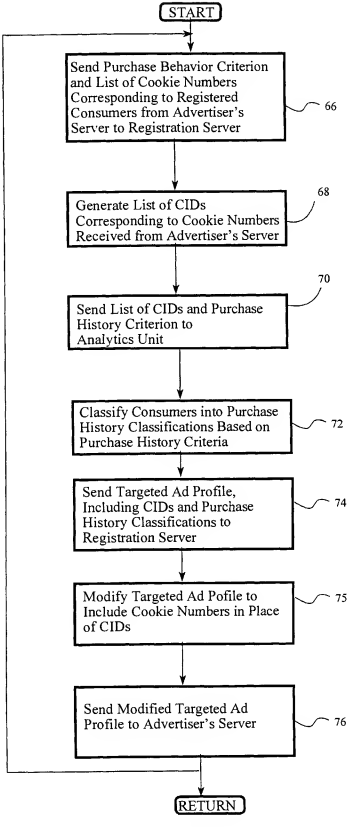

START
Send Purchase Behavior Criterion and List of Cookie Numbers Corresponding to Registered Consumers from Advertiser's Server to Registration Server
66
Generate List of CIDs Corresponding to Cookie Numbers Received from Advertiser's Server
68
Send List of CIDs and Purchase History Criterion to Analytics Unit
70
Classify Consumers into Purchase History Classifications Based on Purchase History Criteria
72
Send Targeted Ad Profile, Including CIDs and Purchase History Classifications to Registration Server
74
Modify Targeted Ad Pofile to Include Cookie Numbers in Place of CIDs
75
Send Modified Targeted Ad Profile to Advertiser's Server
76
RETURN

Figure 8

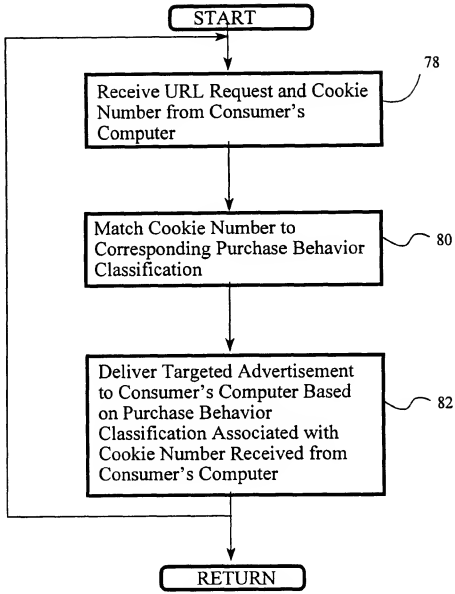

START
Receive URL Request and Cookie Number from Consumer's Computer
78
Match Cookie Number to Corresponding Purchase Behavior Classification
80
Deliver Targeted Advertisement to Consumer's Computer Based on Purchase Behavior Classification Associated with Cookie Number Received from Consumer's Computer
82
RETURN

Figure 9

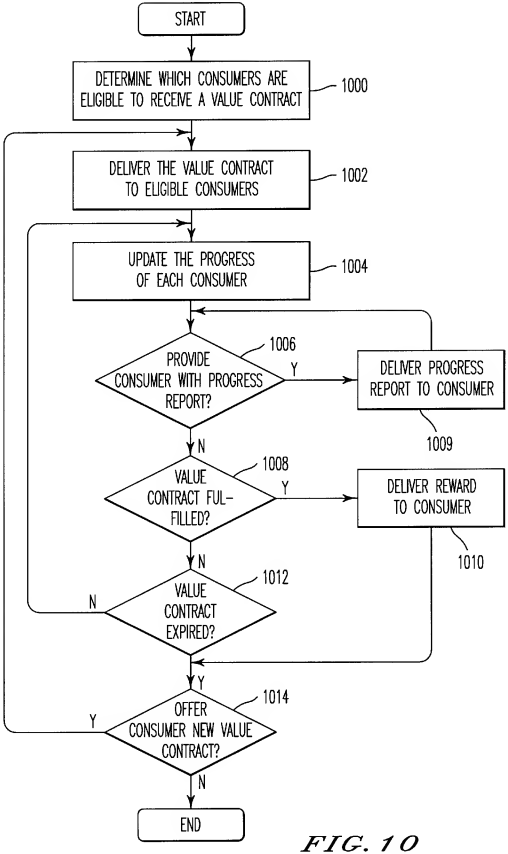

START
DETERMINE WHICH CONSUMERS ARE ELIGIBLE TO RECEIVE A VALUE CONTRACT
1000
DELIVER THE VALUE CONTRACT TO ELIGIBLE CONSUMERS
1002
UPDATE THE PROGRESS OF EACH CONSUMER
1004
PROVIDE CONSUMER WITH PROGRESS REPORT?
1006
Y
DELIVER PROGRESS REPORT TO CONSUMER
1009
N
VALUE CONTRACT FULFILLED?
1008
Y
DELIVER REWARD TO CONSUMER
1010
N
VALUE CONTRACT EXPIRED?
1012
N
Y
OFFER CONSUMER NEW VALUE CONTRACT?
1014
Y
N
END

FIG. 10

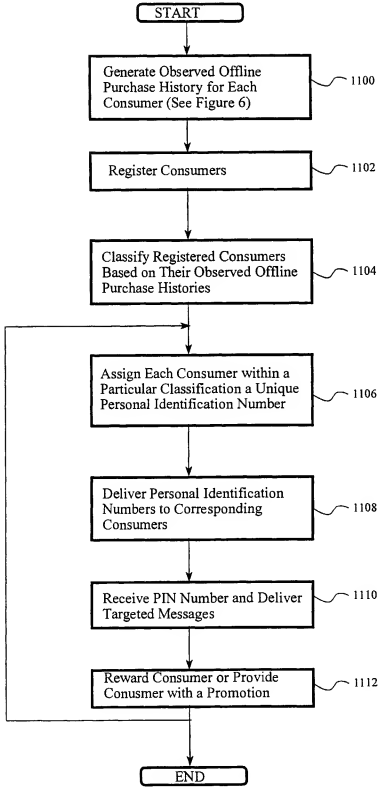

START
Generate Observed Offline Purchase History for Each Consumer (See Figure 6)
1100
Register Consumers
1102
Classify Registered Consumers Based on Their Observed Offline Purchase Histories
1104
Assign Each Consumer within a Particular Classification a Unique Personal Identification Number
1106
Deliver Personal Identification Numbers to Corresponding Consumers
1108
Receive PIN Number and Deliver Targeted Messages
1110
Reward Consumer or Provide Conusmer with a Promotion
1112
END

Figure 11

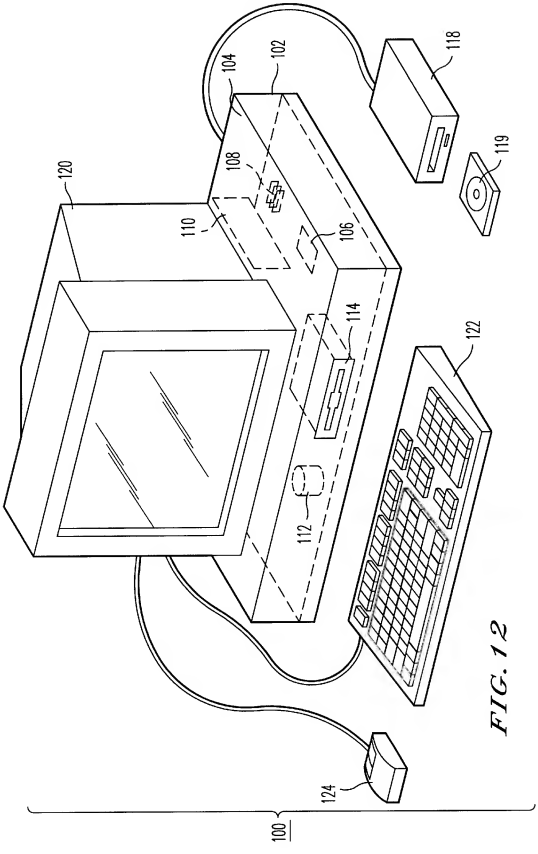


FIG. 12

COMMUNICATING WITH A COMPUTER BASED ON AN UPDATED PURCHASE BEHAVIOR CLASSIFICATION OF A PARTICULAR CONSUMER

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority from U.S. Provisional Application Ser. No. 60/114,462, filed Dec. 30, 1998, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates generally to the use of a computer network, and more specifically to a method, system, and computer program product for communicating with a computer associated with a particular consumer, based on the consumer's offline purchase history.

As used herein, the term "online" refers to activity having at least one aspect that is performed over a computer network, whereas the term "offline" refers to customer activity that is generally not performed over a computer network. For example, using a computer to buy books over the Internet is an online purchase, whereas buying groceries in a grocery store is an offline purchase.

2. Discussion of the Background

With the proliferation of computer networks such as the Internet, more and more households are able to access wide varieties of information quickly and easily with their home (or work) computers. The increasing number of ordinary consumers who are now accessing the Internet has opened up a new avenue through which commercial entities can deliver their advertisements to consumers. Through computer networks such as the Internet, advertisers are able to display banners to computer users for purposes of generating brand name recognition, distributing promotional information, etc.

As evidenced by the numerous amount of literature in the field, skilled computer programers have developed and refined a variety of methods for accessing, manipulating, and disseminating database information over computer networks such as the Internet. Thus, various methods of storing, delivering, and displaying information are well-known in the field of computer networking. Similarly, standard protocols and architecture have been developed to communicate over wide area networks (WANs); for example, TCP/IP protocols and architecture have been developed for communication over the Internet. Moreover, various languages such as Java Database Connectivity (JDBC) have been developed for performing database operations over computer networks. The design and implementation of various methods of database networking and Internet communications are described in Liu et al., "Managing Internet Information Services," O'Reilly & Associates, Inc., 1994; Comer, "Internet Working with TCP/IP Volume I: Principles, Protocols, and Architecture," 2nd ed., Prentice-Hall, Inc., 1991; Comer and Stevens, "Internet Working with TCP/IP Volume II: Design, Implementation, and Internals," Prentice-Hall, Inc., 1991; Corner and Stevens, "Internet Working with TCP/IP Vol. III: Client-Server Programming and Applications," Prentice-Hall, Inc., 1993; Khoshafian et al., "A Guide to Developing Client/Server SQL Applications," Morgan Kaufmann Publishers, Inc.; Hamilton et al., "JDBC Database Access with Java, A Tutorial and Annotated Reference," Addison-Wesley Pub. Co., 1997; and Francis et al., "Professional Active Server Pages 2.0," Wrox Press Ltd., 1998; each of which is incorporated herein by reference.

Currently, advertisers are able to implement a limited form of targeted advertising over the Internet. This is accomplished by sending a block of data, such as a "cookie," from a remote host or server (i.e., a Web server) maintained by an advertiser to a computer (i.e., a client system) that has access to the remote server via the World Wide Web. A cookie, as used in network and Internet communication, is a block of data or state object that a Web server stores on a client system. When the client system accesses a Web site within a limited range of domain names, the client system automatically transmits a copy of the cookie to the Web server that serves the Web site. The cookie may include a unique cookie number corresponding to the client system. Thus, the cookie can be used to identify the client system (by identifying the Web browser) and to instruct the server to send a customized copy of the requested Web page to the Web browser.

Since cookies are also used to track a consumer's online activity, a Web server can deliver targeted advertisements to a consumer's Web browser, based on the consumer's online activity. For example, if a cookie tracks the various IP addresses accessed by the consumer's computer, the Web server can deliver ad banners to the consumer's Web browser based on the IP addresses the Web browser has accessed. Thus, the cookie can be used to record the online activity of a consumer, and information regarding the consumer's tastes and tendencies can be inferred from the consumer's online activity. Using this inference, an advertiser can try to target specific advertisements to specific computer consumers, based on the record of the computer consumers' online activities. That is, the advertiser can try to expose the computer consumers to advertisements designed to appeal to their particular tastes and interests.

The targeted advertisement can be implemented in several manners. For example, the advertiser can generate Internet banners that contain targeted ads and are visible to the consumer when the consumer accesses the advertiser's server, and/or the advertiser can automatically generate e-mail messages and send them to the consumer if the advertiser has the consumer's e-mail address.

The disadvantage of generating advertisements based on online activity resides in the fact that a consumer's actions on the Internet (which are known to advertisers because of the cookie sent to the consumer's computer) may not be strongly related to the consumer's preferences as a consumer in the offline world. Thus, a consumer's activity on the Internet, including online purchases and access to various Web sites, may not reflect what the consumer will buy at a shopping mall or supermarket. For example, just because the consumer has accessed a large number of IP addresses corresponding to fly fishing Web pages, there is no indication that the consumer prefers one brand of diet soda over any other.

SUMMARY OF THE INVENTION

Accordingly, one object of this invention is to provide a novel method, system, and computer program product for delivering targeted advertisements to a consumer based on his or her offline purchase history.

It is another object of the present invention to provide a novel method, system, and computer program product for associating a consumer's offline purchase history with a particular computer used by the consumer.

It is another object of the present invention to provide a novel method, system, and computer program product for

providing advertisers with information relating to consumers' observed offline purchase histories without divulging to the advertisers the proprietary information of another, such as the consumers' customer identifications (CIDs).

These and other objects are achieved according to the present invention by providing a novel method, system, and computer program for delivering a targeted advertisement. The targeted advertisement is selected based on a demonstrated purchase behavior of the consumer including an actual, monitored, or observed offline purchase history associated with the consumer. The targeted advertisement is then electronically delivered to a computer associated with the consumer. Thus, with the present invention it is unnecessary to make inferences about the consumer's offline purchase behavior in selecting the targeted advertisement because the targeted advertisement has been selected based on the observed offline purchase history of the consumer.

In an embodiment of the invention, the computer sends a first identifier to an advertiser. The first identifier is preferably a cookie or any other type of identification information which identifies the computer or consumer. The first identifier is also associated with the consumer's observed offline purchase history which permits targeted advertisements to be delivered to the computer in response to receiving the first identifier from the computer. Accordingly, the targeted advertisement may be sent at times when the computer is known to be online. Further, the targeted advertisements may be sent to the computer from various locations and/or devices, including any device capable of receiving the first identifier and identifying the computer.

In another embodiment of the invention, the consumer provides a second identifier to a registration server. The second identifier is preferably a CID, a bar code, or other string of characters or digital information that identifies the consumer. The registration server associates the first and second identifiers by linking the first identifier and the second identifier in a memory. With this embodiment, it is not necessary that the advertiser delivering the targeted advertisements be provided with the second identifier since the registration server use the first identifier to identify the consumer to the advertiser. Thus, if the second identifier is proprietary, it does not have to be shared with the advertiser for the advertiser to deliver targeted advertisements to the consumer.

In yet another embodiment of the invention, the consumer is classified by assigning to the consumer a purchase behavior classification. The purchase behavior classification is based on selected purchase behavior criterion and the consumer's observed offline purchase history. The targeted advertisement is selected based on the purchase behavior classification assigned to the consumer. Thus, an advertiser can select targeted advertisements to deliver based on the consumer's purchase history classifications, and the consumer's observed offline purchase history does not have to be provided to the advertiser for the advertiser to deliver targeted advertisements. Preferably, one or more classifications are stored as data fields in a single record corresponding to the consumer. This record is generically called a "targeted ad profile."

According to a further embodiment of the invention, the targeted advertisement is a promotional incentive generically termed a "value contract." The value contract offers the consumer a reward for complying with a given type of behavior. This behavior may be a predefined change in behavior or continuance of an established behavior. Preferably, the behavior is defined as a minimum number of purchases that must be made within a predetermined time period. Accordingly, it is possible to deliver promotional incentives that are targeted based on the observed offline purchase history of consumers. Further, the delivery of promotional incentives to certain consumers may be avoided. Consumers for which delivery is to be avoided may include consumers who already comply with the behavior or consumers whose purchase histories demonstrate a reluctance to remain loyal to a particular brand. Once a consumer wins a reward, the reward is preferably presented to the consumer in a retail store. Thus, the reward provides an incentive for the consumer to visit the retail store.

In another embodiment, the consumer is reclassified by assigning to the consumer an updated purchase behavior classification. The updated purchase history behavior criterion is based on the selected purchase behavior criterion and the consumer's updated observed offline purchase history. The targeted advertisement (e.g., a value contract) to be delivered is reselected based on the updated purchase behavior classification. Accordingly, the targeted advertisements delivered to the consumer can be updated to reflect changes in the consumer's behavior. Moreover, the effect of different marketing strategies may be monitored by tracking consumers' responses to being presented with different advertisements.

In yet a further embodiment of the invention, the consumer in a particular purchase history classification receives a unique personal identification number (PIN) based on his or her purchase behavior classification. The consumer receives the PIN from a computer generated printout at a cash register, in an e-mail, or off of a personalized Web page, for example. The consumer is also provided with a telephone number of an interactive voice response (IVR) provider. If the consumer telephones the IVR provider and provides his or her PIN to the IVR provider, then a targeted message, such as an IVR message, is initiated. PINs may also be received from a computer operated by the consumer, in which case targeted messages are delivered to the consumer over a computer network. The targeted messages correspond to the purchase behavior classifications of consumers and include targeted advertisements, promotional offers, and/or instructions on how to receive a reward. If desired, consumers are rewarded for providing their PINs and receiving targeted messages.

BRIEF DESCRIPTION OF THE DRAWINGS

A more complete appreciation of the invention and many of the attendant advantages thereof will be readily obtained as the same becomes better understood by reference to the following detailed description when considered in connection with the accompanying drawings, wherein:

FIG. **1** is a block diagram illustrating a system for associating a consumer's computer with his offline purchase history and delivering targeted advertisements to the consumer over a computer network;

FIG. **2**(*a*) is a drawing of a data structure for storing the offline purchase history of a particular consumer in the purchase history database **8** of FIG. **1**;

FIG. **2**(*b*) is a drawing of a data record for recording purchase information associated with a single purchase in the data structure of FIG. **2**(*a*);

FIG. **3** is a drawing of a data structure for storing a table of first identifiers (cookie numbers) associated with second identifiers (CIDs) in the registration server **14** of FIG. **1**;

FIG. **4**(*a*) is a drawing of a targeted ad profile implemented as a data structure and stored in the advertiser's server **18** of FIG. **1**;

FIG. **4**(*b*) is a drawing of a data structure for storing a unique personal identification number in association with a CID.

FIG. **5** is a flowchart showing the general process for implementing the present invention with the system of FIG. **1**;

FIG. **6** is a flowchart showing how the purchase history database may be populated with the observed offline purchase histories of consumers;

FIG. **7** is a flowchart showing how consumers may register according to the present invention;

FIG. **8** is a flowchart showing how registered consumers may be classified according to their observed offline purchase histories;

FIG. **9** is a flowchart showing how targeted advertisements may be delivered to registered consumers;

FIG. **10** is a flowchart showing how a value contract may be implemented in accordance with the present invention; and

FIG. **11** is a flowchart showing how the present invention may be used to send targeted interactive voice response messages to consumers;

FIG. **12** is a schematic diagram of a general purpose computer system **100** that can be programed to perform the special purpose function(s) of one or more of the devices shown in the system of FIG. **1**.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, wherein like reference numerals designate identical or corresponding parts throughout the several views, and more particularly to FIG. **1** thereof, a system illustrative of the present invention is shown. The system includes stores **2**, **4**, **6**; a purchase history database **8**; a first computer **10**; a telephone **11**; a second computer **12**; a registration server **14**; an analytics unit **16**; an advertiser's server **18**; a wide area network (WAN) such as the Internet **20**; various computers linked to the Internet **20**, such as Web servers **22**, **24**, and computers **26**, **28**, for example; and an interactive voice response (IVR) provider **29**.

Each customer or consumer is provided with a customer identification (CID) that identifies the particular consumer. The CID can be any identifier that is scanned, read, or otherwise entered into a computer system at checkout. Preferably, the CID is represented as a bar code so that it can be quickly scanned at checkout, although any other type of machine-readable (or non-machine readable) implementations for storing or displaying identifications may be used, including magnetic strip and computer or memory chips on a card (e.g., smart cards). Examples of possible CIDs are credit card numbers, debit card numbers, social security card numbers, driver's license numbers, checking account numbers, street addresses, names, e-mail addresses, telephone numbers, frequent customer card numbers, shopper card identifications (SCIDs), or shopper loyalty card numbers issued by one of the stores **2**, **4**, and/or **6**, although any suitable form of identification may be used.

The stores **2**, **4**, **6** may be any retail location, point of sale, or other location in which offline transactions are made by consumers. The stores **2**, **4**, **6** record purchase data for the consumers that present their CIDs at checkout. The purchase data includes information such as the location of the purchase, the items purchased, the price of each item purchased, and CID. The purchase information can be stored electronically in a general purpose computer in each of the stores **2**, **4**, **6** and sent to the purchase history database **8** periodically, in real time, or at any other time when it is desirable to update the purchase history database **8**.

The purchase history database **8** may be implemented using any desired structure including any type of computer connected to any type of storage device including magnetic disks such as one or more hard disk drives, optical disks, magneto-optical disks, memory chips, or other desired storage devices. The purchase history database **8** stores purchase data received from the stores **2**, **4**, **6**. The purchase data may be stored in separate master records for each consumer, as described below with reference to FIGS. **2**(*a*) and **2**(*b*). U.S. Pat. Nos. 5,832,457, 5,649,114, 5,430,644, and 5,592,560 describe techniques for collecting consumer purchase information and for storing such information in a purchase history database **8**. U.S. Pat. Nos. 5,832,457, 5,649,114, 5,430,644, and 5,592,560 and all references cited therein are incorporated herein by reference. Additionally, techniques for collecting consumer purchase information and for storing such information in a purchase history database **8** are described in other patents owned by Catalina Marketing and/or Catalina Marketing International. Each patent owned by Catalina, Catalina Marketing, and/or Catalina marketing international is incorporated herein by reference.

The first and second computers **10**, **12**, the registration server **14**, the advertiser's server **18**, Web servers **22**, **24**, and computers **26**, **28** may each be implemented as a general purpose computer (e.g., the computer **100** of FIG. **12**). The first and second computers **10**, **12**, the registration server **14**, the advertiser's server **18**, Web servers **22**, **24**, and computers **26**, **28** may be appropriately programmed to communicate with one another over a wide area network (WAN) such as the Internet **20**.

The first and second computers **10**, **12** may be any computer that one or more consumers can access, such as home or office computers. The first and second computers **10**, **12**, may also be implemented as interactive television sets or other structure suitable for receiving interactive advertisements. Interactive television systems are described in U.S. Pat. Nos. 4,847,700, 5,721,583, and 5,552,735. U.S. Pat. Nos. 4,847,700, 5,721,583, and 5,552,735 and all references cited therein are incorporated herein by reference. The first and second computers **10**, **12** may be programmed with any suitable Web browser software that permits the first and second computers **10**, **12** to retrieve Web pages via the Internet **20** from remote computers or servers such as the advertiser's server **18** and/or the registration server **14**. The Web browser software may also be used to transmit registration information provided by a consumer to a remote computer such as the advertiser's server **18** and the registration server **14**.

The registration server **14** is a Web server programmed to receive, store, and/or transmit various type of information, including registration information, purchase behavior information, and information for identifying consumers, although the registration server may also be implemented using any type of computer. The registration server **14** may additionally be programmed to generate records that link various types of registration information received from consumers and the advertiser's server **18**.

The analytics unit **16** may be implemented using any desired structure such as a computer programmed to analyze purchase data (e.g., master records) received from the purchase history database **8**. Thus, the analytics unit **16** may be programmed to receive purchase behavior criteria from a

remote computer (e.g., the registration server **14** and/or the advertiser's server **18**) and apply those criteria to the purchase data in the purchase history database **8** to classify consumers into one or more purchase behavior classifications. As shown, the analytics unit **16** communicates directly with the purchase history database **8**, the registration server **14**, and the IVR provider **29**; however, the analytics unit **16** may also be connected to other remote computers (e.g., the advertiser's server **18**) directly, via the Internet **20**, or through any network.

The advertiser's server **18** may be a Web server programmed to send and receive registration information to and from a remote computer such as the first computer **10**. The advertiser's server **18** may also be programmed to exchange information with the registration server **14**, to associate a remote computer with one or more registered consumers, and to deliver targeted advertisements over the Internet to remote computers such as the first and second computers **10**, **12**. Different types of targeted advertisements, include Internet banners, real time moving videos, video information, animation information, audio information, online interstitial advertisements, electronic mailings (e-mails), interactive television advertisements, and any other type of message, recording, and/or display.

The Internet **20** includes various networks and gateways for linking together various computer networks and computers such as the first and second computers **10**, **12**, Web servers **22**, **24**, and computers **26**, **28**. The advertiser's server **18**, the Web server **22**, and/or the Web server **24** may be appropriately programmed with server software for delivering Web pages to remote clients or computers such as the first and second computers **10**, **12**. The Web servers **22**, **24** may be any servers connected to the Internet **20**, including servers that are maintained by one or more advertisers and programmed to deliver targeted advertisements to consumers via the Internet **20**. Likewise, the computers **24**, **26** may be any server or client with access to the Internet **20**. Thus, the computers **26**, **28** may be home computers on which consumers may register with the registration server **14** or Web servers programmed to function similar to the registration server **14** or the advertiser's server **18**.

The IVR provider **29** is any system that includes at least one computer programmed to store and play IVR messages to consumers. The IVR provider **29** exchanges information with the analytics unit **16**. Consumers use a telephone **11**, for example, to provide inputs to the IVR provider and receive IVR messages from the IVR provider. The telephone **11** is any device suitable for sending inputs (such as voice or touch tone commands) and receiving IVR messages.

It is emphasized that the system of FIG. **1** is for exemplary purposes only, as many variations of the hardware used to implement the present invention will be readily apparent to one having ordinary skill in the art. For example, the analytics unit **16** may incorporate the purchase history database **8**. As another example, the registration server **14** may incorporate the advertiser's server **20**. To implement these variations as well as other variations, a single computer (e.g., the computer **100** of FIG. **12**) may be programmed to perform the special purpose functions of two or more of any of the devices shown in FIG. **1**. On the other hand, two or more programmed computers may be substituted for any one of the devices shown in FIG. **1**.

The present invention stores information relating to each consumer's observed offline purchase history and identifying information corresponding to each consumer in one or more memories such as a hard disk, optical disk, magneto-optical disk, and/or RAM, for example. The stored information may include the purchase history, CID, cookie number, and targeted ad profile for each consumer. One or more databases may store the information used to implement the present invention. The databases are organized using data structures (e.g., records, tables, arrays, fields, and/or lists) contained in a memory such as a hard disk, floppy disk, optical disk, or RAM, for example.

FIG. **2**(*a*) shows a master record **30** for storing purchase information for a particular CID corresponding to a particular consumer. A separate master record **30** for each CID is maintained in the purchase history database **8**. The master record **30** may be implemented as a data structure that includes a field **31** for storing the consumer's CID as well as a table **32** for identifying and describing each purchase made by the consumer. The table **32** may include one or more linked lists, for example, or an array of purchase records.

FIG. **2**(*b*) shows an exemplary purchase record **33** which may be implemented as part of the master record **30**. The purchase record **33** includes a field **34** for indicating the shelf keeping unit (SKU) which is a distinct product such as "one 2 liter bottle of Brand Z soda," a field **35** for the universal product code (UPC) which is usually seen as a bar code on a product, a field **36** for the location of the purchase, a field **37** for the price per SKU, and a field **38** for the date of purchase. Additional fields and/or columns may be added to the purchase record **33** as desired. Preferably, the master record **30** and/or the purchase record **33** contain at least the information used by the analytics unit **16** to identify or classify consumers, as will be described below with reference to FIG. **8**.

FIG. **3** illustrates an association table **40** for storing information that associates a computer with a particular consumer and master record. The association table **40** may be implemented as a data structure including a list **42** of first identifiers linked to a list **44** of second identifiers. As shown, the list **42** is a list of cookie numbers. Each cookie number corresponds to a cookie that has been sent to a computer as a result of a consumer registering online with the registration server **14** (described below with reference to FIG. **7**). Accordingly, each cookie number identifies a single Web browser run on a computer that was used by a consumer to register. The list **44** is a list of CIDs, each of which corresponds or is linked to the adjacent cookie number in the list **42**. Each CID in the list **44** is also stored in the purchase history database **8** in a master record. Thus, the association table **40** links a Web browser (via the cookie number) with a master record (via the CID) for a consumer who used the Web browser to register online. The association table **40** may be stored in the registration server **14** or any other suitable storage device including any of the devices shown in FIG. **1** (e.g., the registration server **18**). As technology progresses, cookies may become associated with individuals and not directly correspond to a Web browser, and the invention includes the use of identification methods other than conventional cookies.

The association table **40** may contain additional lists and/or fields. For example, it may be desirable for the association table **40** to include a field that identifies the association table **40** if multiple association tables are generated and stored. Preferably, the association table **40** stores at least one list of identifiers which are also stored in the purchase history database **8** and which identify registered consumers.

FIG. **4**(*a*) is an exemplary targeted ad profile **446** for storing information relating to a consumer's purchase

behavior classification. The targeted ad profile **446** may be a data structure that includes a record having a field **448** for identifying the consumer. As shown, the field **448** stores the cookie number associated with the consumer. The targeted ad profile **446** may include additional fields for storing the consumer's purchase behavior classification with regard to one or more purchase behavior criterion. The targeted ad profile **446** includes three fields, **449***a*, **449***b*, and **449***c*, for three purchase behavior classifications: Brand Z loyalty, Heavy Snacker, and Healthy Household, respectively. Each purchase behavior classification may be given any score (e.g., an integer), a describer (e.g., "Brand Z loyalist" or "Heavy Brand Z User"), flag ("1" or "0"), or rank (e.g., "50th out of 50,000) that the consumer has received based on selected purchase behavior criteria which are discussed below with reference to FIG. **8**.

The targeted ad profile **446** is preferably generated by the analytics unit **16** or another device in close proximity to the purchase history database **8**. However, the targeted ad profile may be generated by any suitable device including any of the other devices shown in FIG. **1** (e.g., the registration server **14**). If desired, multiple targeted ad profiles may be generated for each consumer. Also, the targeted ad profiles may be updated as often as desired to capture consumers' behavioral changes, i.e., changes in purchase behavior classifications.

FIG. **4**(*b*) shows a data structure **460** that includes a field **470** for storing information identifying a particular targeted message such as an IVR message stored in the IVR provider **29**. An IVR message includes one or more recorded voice messages that are played for a consumer. Different messages may be played in response to inputs received from the consumer over a telephone network. The input may include information that is delivered orally or by touch tone. For example, the IVR message may begin by playing the consumer a message that states, "Speak or press '1' if you prefer brand X over brand Y; speak or press '2' if you prefer brand Y, but would be willing to try brand X." Thus, a single IVR message may include numerous sequences and/or variations of recordings to be played to the consumer, and the input received from the consumer at each prompt determines which particular recordings of the IVR message are played to the consumer.

The data structure **460** also includes a field **480** for storing a list of PINs associated with the IVR message stored in field **470**. The PINs may include numbers but should not be limited to numbers and may include, if desired, alphabetic, typographic, or any type of identifying information including CIDs, telephone numbers, cookie numbers, any personal attribute such as voice, fingerprint, or facial characteristics, and random strings of alphanumeric characters. The data structure **460** is generated in the analytics unit **16** and sent to the IVR provider **29** so that the IVR provider **29** can receive a PIN from a consumer and play the corresponding IVR message. Multiple data structures such as the data structure **460** can be generated so that different IVR messages correspond to different lists of PIN numbers. Each IVR message is associated with a particular purchase history classification so that each consumer hears an IVR message that reflects his or her offline purchase history.

The data structures embodied by the present invention include the data structures shown in FIGS. **2**(*a*), **2**(*b*), **3**, **4**(*a*), and **4**(*b*) and described above. Alternatively, any other desired manner of implementing the data structures embodied by the present invention may be equivalently implemented so that the desired functionality and corresponding practical application are achieved.

FIG. **5** is a flowchart that shows the general process for implementing the invention. Each of the steps of FIG. **5** includes two or more substeps which are described below with reference to FIGS. **6**, **7**, **8**, and **9**.

Referring back to FIG. **5**, the purchase history database **8** is populated with the actual, monitored, or observed offline purchase histories of consumers in step **500**. Further details of this step are described below with respect to FIG. **6**. The offline purchase histories are organized into master records, each corresponding to a CID or other identifier associated with a particular consumer.

In step **502**, each consumer registers online using a computer. As a result of the registration process, each computer is associated with the offline purchase history of the consumer that used the computer to register. Further details of step **502** and the registration process are set forth below in the description of FIG. **7**.

In step **504**, the registered consumers are classified by assigning each consumer a purchase behavior classification. The purchase behavior classification is assigned to each consumer according to predefined purchase behavior criteria applied to the consumer's observed offline purchase history. Further details of this step are set forth in the description of FIG. **9**.

In step **506**, targeted advertisements are electronically delivered to the respective computers of registered consumers. The targeted advertisements are selected based on the purchase behavior classification assigned in step **504**. Thus, a first consumer using the first computer **10** may receive an advertisement different from the one received by a consumer using the second computer **12**. The difference in the advertisements will be, at least in part, caused by differences in the first and second consumer's respective purchase behavior classifications. Further details of step **506** are described with respect to FIG. **506**.

FIG. **6** is a flowchart of the process of step **506** of FIG. **5** and shows how consumers' offline purchase histories are observed, recorded, and updated. After starting, in step **50**, the consumer's offline purchase information is obtained. This information is obtained in the preferred embodiment by a computer used to implement a sale or sales transaction to a user and may utilize a general purpose computer or point of sale terminal. If a point of sale terminal is used, the purchase history may be obtained using an optical scanner which scans a bar code, UPC code, or SKU on the purchased product.

In step **51**, the consumer's observed offline purchase information is received in the purchase history database **8**. The observed offline purchase information can be delivered from the stores **2**, **4**, **6**, to the purchase history database **8** via any suitable means, such as an electronic communications network or physical delivery of computer diskettes, tapes, or other portable media containing the purchase information, for example.

In step **52**, a master record corresponding to the consumer is created based on the offline purchase information received in step **51**. The master record contains at least one identifier, such as the consumer's CID, that distinguishes the consumer's master record **30** from other master records in the purchase history database **8**. Steps **50**, **51**, and **52** may be repeated as necessary to generate master records for additional consumers, as well as to update existing master records by appending new information to an existing master record.

FIG. **7** is a flowchart showing how the registration process of step **504** is performed. In step **54**, the consumer uses Web browser software on the first computer **10** to initiate the registration process. Registration is initiated by the consum-

er's selection of a button or other graphic image on a Web page associated with the advertiser's server **18**.

Then, in step **56**, the advertiser's server **18** sends a cookie to the first computer **10**. A cookie is a block of data, a state object, or identification information. The cookie sent to the first computer **10** includes a unique identifier, such as a cookie number or other string of characters, that is stored on the first computer **10** and at the advertiser's server **18**. When the Web browser running on the first computer **10** accesses the advertiser's server **18**, the Web browser sends a copy of the cookie, including the cookie number, back to the advertiser's server **18**. In this manner the advertiser's server recognizes the cookie as being sent from a particular Web browser program associated with a particular consumer. Since the same cookie may be sent to, and recognized by, any server within a predefined range of domain names, other servers, such as Web servers **22**, **24**, may receive and recognize the cookie (as well as the cookie number) stored in the first computer **10** if the other servers have domain names in the requisite range. In an alternate embodiment, instead of identifying the Web browser program, the identification information may be used to identify the computer of a consumer and/or the consumer himself.

In step **58**, the cookie number is sent from the advertiser's server **18** to the registration server **14**. The cookie number may be sent from the advertiser's server **18** to the registration server **14** by placing the cookie number in a URL (Uniform Resource Locator) statement. Thus, a cookie can be assigned when a first Web page provided by the advertiser's server **18** is requested by the first computer **10**. The first Web page can contain a link to a second Web page provided by the registration server **14**. When the consumer selects the link to the second Web page, the cookie number can be placed in the URL statement for the second Web page, and thus sent to the registration server **14**.

In step **60**, the consumer's Web browser jumps to a registration Web page served by the registration server **14**. Then, in step **62**, the consumer registers online with the registration server **14** and, in the process, provides the registration server **14** with information, including an identifier found in the master record **30** (e.g., the consumer's CID). The consumer may supply the registration server **14** with information about the consumer to generate an online profile for the consumer. The online profile may include information such as the consumer's name CID, e-mail address, product/brand preferences, demographic information, work address, home address, whether the consumer has any babies, and whether the consumer has any pets such as a cat, dog, bird, or fish. Preferably, the online profile includes at least one item of information that is stored (or is to be stored) in the purchase history database **8**. While referred to as an online profile, the profile may be generated or obtained on an offline basis, such as by filling out a card in a grocery store, for example. Other forms of registration may include a consumer entering registration information at a kiosk in the grocery store after scanning the bar code or alternatively swiping the magnetic strip of his or her shopper loyalty card through a magnetic strip reading device. The profile preferably includes information of how to transmit by computer information to the consumer, such as the consumer's e-mail address, IP (Internet protocol) address, or any information which may be used to electronically send information to the consumer, including, for example, through a paging device or a portable computer.

In step **64**, the registration server **14** stores the cookie number received from the advertiser's server **18** and the CID received from the first computer **10** in memory and links the cookie number to the CID. Accordingly, an association between the consumer, the consumer's CID, and the first computer **10** results. Once the cookie number and CID are linked, the registration server **14** can use a cookie number to locate a particular master record in the purchase history database **8** based on the CID linked to that cookie number. Further, the registration server **14** can use a cookie number to identify a particular consumer to an advertiser without divulging the consumer's CID.

Accordingly, after steps **54** through **64** have been performed, the consumer has completed registration with the system. Additional consumers may register in the same manner as described in steps **54** through **64** so that a list of cookie numbers and associated CIDs is generated for the registered consumers. The list of cookie numbers and the list of CIDs may be stored in the fields **35** and **36**, respectively, of the association table **40** of FIG. **3**.

Different servers, such as Web servers **22**, **24**, including the registration server **14**, may be programmed to perform the same function as the advertiser's server **20**, and thus, servers other than the advertiser's server **20** may be used to initiate registration in steps **54** through **58**. Accordingly, the registration server **14** may store one or more association tables corresponding to different lists of cookie numbers generated by different servers in steps **54** through **58**. Preferably, the master records for each consumer continue to be updated after registration to track the consumers' offline purchases and changes in purchase behavior.

FIG. **8** is a flowchart showing how consumers are classified into one or more purchase behavior classifications based on their observed offline purchases and corresponds to step **506** of FIG. **5**. In step **66**, the advertiser's server **18** sends to the registration server **14** selected purchase behavior criteria and a list of cookie numbers corresponding to consumers who have registered through the advertiser's server **18**. The purchase behavior criteria may be selected using any suitable technique for classifying consumer's observed purchase behavior. Possible techniques for determining purchase behavior criteria include pattern classification, cluster analysis, the use of criteria arbitrarily set by a marketing expert, and/or any other method of classifying consumers into one or more behavioral groups based on their observed offline purchase history. For example, the criterion for a class of "heavy Brand Z drinkers" may be defined as any consumer who has purchased Brand Z at least twice a year in the last month. As another example, the criterion for a class of "Brand Z loyalists" may be defined as any consumer who has purchased Brand Z at least once a month for the last nine months. Regardless of how different criteria are determined, the criteria are preferably based on information derived from marketing research. The purchase behavior criteria do not necessarily have to originate from the advertiser's server **18**, but may originate from any suitable remote device such as the computer **26**, the Web server **24**, and/or the registration server **18**.

In step **68**, the registration server **14** generates a list of CIDs corresponding to the cookie numbers received from the advertiser's server **18**. Thus, step **68** is a matching step in which the registration server identifies a subset of the total number of CIDs to be analyzed in the purchase history database **8**. The registration server **14** may use the association table **40** generated in step **64** to identify the CIDs that correspond to the cookie numbers received in step **66**.

Next, in step **70**, the registration server **14** sends to the analytics unit **16** the purchase behavior criteria received in step **66** and the list of CIDs generated in step **68**.

In step **72**, the analytics unit **16** analyzes the master records corresponding to the list of CIDs to classify the respective consumers into one or more purchase behavior classifications based on the purchase behavior criteria.

In step **74**, the analytics unit **16** sends to the registration server targeted ad profiles for each consumer identified in step **68**. Each of the targeted ad profiles includes the consumer's CID and the purchase behavior classification(s) corresponding to that CID. The targeted ad profiles may be stored in a table such as an array or table of records, linked lists, or other suitable data structure.

In step **75**, the registration server **14** modifies the targeted ad profiles received from the analytics unit **16** so that the CID for each targeted ad profile is replaced with the corresponding cookie number. To perform this function, the registration server uses the association table **40** to identify the cookie number corresponding to each CID.

In step **76**, the registration server **14** sends the modified targeted ad profiles received from the analytics unit **16** to the advertiser's server **20**. As discussed above, each targeted ad profile contains the cookie number and the purchase behavior classification(s) associated with a particular consumer. Information, including targeted ad profiles, received from the analytics unit **16** by the registration server **14** may sent to the advertiser's server **20** via any appropriate method, for example, over the Internet **18** or physically delivered on a portable computer readable medium.

Accordingly, in steps **66** through **76**, the actual or observed purchase history of the consumers in the purchase history database **8** is analyzed, based on selected purchase behavior criteria, to identify a list of cookie numbers corresponding to consumers who meet the preselected purchase behavior criteria. Steps **66** through **76** may be repeated as necessary so that any number of servers maintained by various advertisers can provide the analytics unit **16** with purchase behavior criteria and cookie numbers of registered consumers (step **66**) and receive targeted ad profiles or other purchase behavior information from the analytics unit **16** (step **76**).

As demonstrated by the process shown in FIG. **8**, advertisers who maintain servers other than the registration server **14** may be provided with targeted ad profiles without being provided with any of the data stored in the purchase history database **8**, including CIDs, the consumers' identities, and their observed purchase histories. Thus, if the operator of the registration server **14** is contractually bound to the stores **2**, **4**, **6** to maintain the consumers' CIDs in secrecy, then the invention may still be practiced without violating the contract and without transmitting the CID.

FIG. **9** is a flowchart showing how targeted advertisements are electronically delivered to consumers and corresponds to step **506** of FIG. **5**. In step **78**, the consumer who was registered by the system in steps **54** through **64** uses the Web browser running on the first computer **10** to make a URL request to a Web site served by advertiser's server **18**. Since the advertiser's server **18** has a domain name in the range specified by the cookie sent in step **56**, the Web browser will send a copy of the cookie, including the cookie number, to the advertiser's server **18** along with the URL request.

In step **80**, the advertiser's server **18** matches the cookie number received from the first computer **10** to the modified targeted ad profile associated with the cookie number. Then, in step **80**, the advertiser's server **18** delivers an advertisement to the first computer **10** based on at least one of the purchase behavior classifications stored in the targeted ad profile. In addition to the advertiser's server **18**, any host computer or server (for example, Web servers **22**, **24**, the registration server **14**, and/or computers **26**, **28**) having a domain name within the requisite range defined by the cookie may be programmed to perform steps **78** through **82**.

Steps **78** through **82** may be repeated every time a registered consumer uses his or her computer to send a URL request for a Web site served by a Web server that has taken part in the registration process (steps **54** through **76**) in the same manner as the advertiser's Web server **18**. As noted above, a consumer's online activities may not reveal, or may even contradict, a consumer's offline purchase behavior. The present invention overcomes many of the drawbacks of conventional online advertising by delivering targeted advertisements that are based on what consumers are known to have purchased offline, i.e., their observed offline purchase histories.

Thus, in steps **78** through **82**, targeted advertisements are delivered online to the consumer based on the consumer's observed or actual offline purchase behavior. Further, it is not necessary to provide an advertiser with the data in the purchase history database **8** for the advertiser to deliver targeted advertising based on the consumer's observed offline purchase history.

Any variety of targeted advertisements can be delivered to the home computer **12** of the consumer. For example, the advertisements might be for product offers that are only good at stores, such as stores **2**, **4**, **6**, that provide purchase information to the purchase history database **8**. In this manner, retail locations, such as stores **2**, **4**, **6**, that are willing to provide purchase data to the purchase history database **8**, are rewarded by having their stores' names explicitly mentioned in the targeted advertisements delivered to the consumer. Moreover, if the banner ads are only good at stores where the consumer is known to shop (based on the information in the master record associated with the consumer), then participating stores can be assured that the targeted advertisements will not be used to encourage the consumer to shop at competing stores. For example, the master records for a first consumer and a second consumer show that the first consumer prefers to shop at store **4** and the second consumer prefers to shop at store **6**. The analytics unit **16** may be programmed to place the first and second consumers in different purchase behavior classifications, based on their preferred store (among other things). Accordingly, the classifications can be used by the advertiser's server **18** to deliver targeted promotions or coupons that are only recognized at the store where each consumer prefers to shop.

One type of targeted advertisement that can be delivered in step **82** is a value contract. The value contract is a promotional incentive in which the consumer is offered a reward for complying with a particular behavioral pattern such as a predefined change in behavior or the continuance of an established behavior. Any type of reward may be offered. The reward may be "points" which may correspond to, or be redeemed for, cash, cash equivalents, frequent flier miles, minutes of long distance time, minutes of Internet service provider time, coupons, discounts, prizes, or free products, for example. The registration server **14** (or any other suitable server) may be programmed to serve customized Web pages to consumers's computers. Such customized Web pages may display such information as a consumer's accumulated points and the various prizes, rewards, etc. that can be "purchased" with the points. The reward may also be an e-mail message with a password for a Web page full of coupons and customized according to the consumer's

observed offline purchase history, for example. The e-mail may also have a link that the consumer can select to start the Internet software on his or her computer and request a customized Web page of coupons.

As discussed above, the value contract may be a promotional incentive for consumers to change existing behavior or continue an established behavior, as determined from the consumer's offline purchase histories. Thus, in order for a consumer to fulfill a value contract and receive a reward, the consumer may be required to purchase a preselected amount of a specified product within a predetermined amount of time. The "amount" of product may be measured by volume, weight, cost, shelf keeping unit (i.e., number of products), or any combination thereof. For example, the value contract may require a consumer to purchase at least 5 pounds of Brand X cheese for a total cost of at least $25 dollars to receive the reward. As another example, a consumer may be required to purchase a total of 10 Brand X cheese products for a total cost of at least $30 to receive the reward.

FIG. **10** is a flowchart showing how a value contract may be implemented. In step **1000**, the analytics unit **16** searches the purchase history database **8** for consumers whose master records indicate that they are eligible for receiving a value contract offer. The eligibility of each consumer may depend on any desired factor(s) including the purpose of the contract, whether the consumer's observed offline purchase history meets certain criteria, and the consumer's response to previously delivered targeted advertisements including value contracts. As an example, assume the value contract will reward consumers who buy Brand Z soda twice a week. In this case, it may not be desirable to offer the value contract to consumers who are known Brand Z fanatics, i.e., consumers whose observed offline purchase histories indicate that they need no incentive to purchase large quantities of Brand Z soda. Therefore, the criteria used to determine the eligibility of consumers may be "any consumers who have made less than twelve purchases of Brand Z soda in the last six weeks," for example. As another example, the criterion may be "any consumers who made less than ten purchases of Brand Z soda, but more than 10 purchases of Brand X soda in the last six weeks."

In step **1002**, the value contract is delivered to the eligible consumers. Step **1002** is analogous to step **506** in FIG. **5**. Therefore, step **1002** may be performed by the advertiser's server **18** or another computer programmed to deliver targeted advertisements, e.g., the registration server **14**. The value contracts may be delivered by e-mail, Internet banners, or any other suitable technique. In a preferred embodiment, the consumer can use a computer to check a particular Web page on which all value contracts for which the consumer is eligible are displayed. In this embodiment, the value contracts may be Internet banners which are automatically sent to the consumer's computer by a Web server upon recognizing the consumer's computer or upon the consumer's entry of a password, for example.

In step **1004**, the analytics unit updates each consumer's progress toward fulfilling the value contract based on the purchase history of the consumer in the purchase history database **8**. The progress may be determined by monitoring the purchases by a particular consumer. The consumer may be identified by a frequent shopper or loyalty card, credit or debit card number, checking account number, or using any other identification. Each time a consumer whose identification can be determined makes a purchase, the items purchased along with the consumer's ID are stored in the purchase history database **8**.

In step **1006**, the registration server **16** determines whether each consumer is to be provided with a progress report which indicates the consumer's progress toward fulfilling the value contract. The progress reports may be provided automatically or may be requested individually by any eligible consumer. For example, e-mails or telephone messages could be automatically generated and sent to the consumers informing them of their progress. Consumers could also be kept abreast of their progress by actively accessing a personalized Web page, calling a predetermined telephone number, and/or by computer generated printout at a point of sale, for example. If the consumer is not to be provided with his or her progress report, then the process proceeds to step **1008**. If the consumer is to be provided with his or her progress report, then the process proceeds to step **1009**.

In step **1009** the registration server **14** or other suitable device (e.g., a computer in the store **4**) delivers the progress report to the consumer. The progress report may be printed at checkout, delivered as an Internet banner by a server that can recognize the consumer's computer, delivered by e-mail, and/or any other suitable method. The message may also offer encouragement, e.g., "Only two more to go. You're almost there!" The consumer may also be provided with ways to check his or her progress toward fulfilling or completing a value club contract by calling a toll free number, checking a particular Web page, suppling his or her CID to a computer terminal in a retail store, and/or any other suitable method. After the consumer is provided with a progress report, the process returns to step **1006**.

In step **1008**, the analytics unit **16** determines, for each consumer, whether the consumer has fulfilled the value contract. This determination is based on the progress check performed for each consumer in step **1004**. If the consumer has not fulfilled the value contract, the process proceeds to step **1012**. If the consumer has fulfilled the value contract, the process proceeds to step **1010**.

In step **1010**, the registration server **14** presents the consumer with a reward for fulfilling the value contract. Delivery of the reward may be conditioned on the behavior of the consumer. For example, acceptance of the reward may require that the consumer to visit a specified retail location such as a specific grocery store. Accordingly, the value contract can be implemented to provide the consumer with an incentive to visit selected locations. The locations may be selected on the consumer's preestablished shopping habits (e.g., the grocery store that the consumer frequents most often), as determined from the master record corresponding to the consumer in the purchase history database **8**. After step **1010**, the process proceeds to step **1014**.

In step **1012**, the analytics unit **16** determines whether the value contract offer is still good or open. If the offer is still open, the process returns to step **1004**. If the offer is no longer good (for example, if the time for fulfilling the contract has expired), then the process proceeds to step **1014**.

In step **1014**, the registration server **14** determines whether a new value contract should be offered to consumers who were offered the original value contract in step **1002**. This determination may be based on such factors as the consumer's response to the original value contract, the consumer's response to other value contracts in the past, and the consumer's observed offline purchase behavior over a certain period of time. Step **1012** is analogous to step **1000** in that criteria may be used to determine wether consumer who were offered the original value contract should be offered a new value contract. If a new value contract is not offered, then the process ends. If a new value contract is

offered, the process returns to step **1002** and the new value contract is delivered.

The conditions of each new value may be different for each consumer who was offered the original value contract. Preferably, the new value contracts are altered for each consumer as each consumer's behavior changes over time. For example, a consumer who has only purchased Brand X soda once in the last six weeks may be offered a first value contract that rewards the consumer for purchasing over two liters of Brand X soda within the next six weeks. If the consumer complies, i.e., the consumer buys over two liters of Brand X soda within six weeks, the consumer may be offered a second value contract that rewards the consumer for purchasing over three liters of Brand X soda within six weeks. If the consumer complies with the second contract, the consumer may be offered a third value contract that rewards the consumer for purchasing six liters of Brand X soda within six weeks.

Thus, as a consumer demonstrates increasing loyalty toward a particular product, the terms of the contract may require that the consumer buy the product more frequently. Likewise, the reward, i.e., the consideration for fulfilling the value contract, may be varied as the consumer's purchase behavior changes. For example, the consumer may be offered a first value contract that requires three purchases of Brand Z cereal, any size, within three weeks. If the consumer complies with the terms of the contract, he or she may be given a ten dollar credit at a particular store. Then, the consumer may be offered a second value contract that requires three purchases of Brand Z cereal within three weeks, but only offered a five dollar credit. If the consumer does not comply with the second value contract, then the consumer may be offered a third value contract that offers an eight dollar reward. The third value contract may also be a modification of the second value contract, e.g., an Internet banner informing the consumer that he or she only has to buy two items of Brand Z cereal to win the five dollar reward. Accordingly, a value contract's reward and/or requirements may be altered to encourage the consumer to continue to engage in desirable behavior and/or to change undesirable behavior. The value contracts, as well as any other targeted advertisements, are preferably updated and/or refined as often as possible to reflect changes in the consumers' observed purchase behaviors over time.

When used as a targeted advertisement, the value contract provides an efficient way to deliver promotional incentives to consumers for whom the promotional incentives will be more meaningful. That is, consumers who already demonstrate desirable purchase behavior, based on their respective master record and/or targeted ad profiles, can be provided with different offers and incentives than consumers who demonstrate purchase behavior which an advertiser wishes to change. It may be undesirable to offer a value contract to consumers who need no reward incentives to comply with the requirements of the value contract, i.e., consumers whose purchase histories indicate that they would fulfill the requirements of the contract without a reward. Also, it may be undesirable to continue to offer rewards to "switchers," i.e., consumers who will buy a particular brand to fulfill certain value contracts but fail to develop a loyalty for that particular brand. The loyalty of a consumer toward a particular brand may be gauged by the consumer's reaction to different incentives—the more loyal the consumer, the smaller the incentive needed to influence the consumer. To encourage continuance of a desired behavior, brand loyalists may be delivered targeted advertisements that provide small rewards for continued loyalty and/or messages that acknowledge and thank the consumer for his or her brand loyalty. On the other hand, consumers who repeatedly resist value contract offers may be offered increasingly higher rewards. Further, consumers who continue to comply with value contracts may be offered decreasingly lower awards.

FIG. **11** is a flowchart that shows a process for sending targeted messages to consumers based on their offline purchase history. Such messages may include interactive voice response (IVR) messages which, as discussed above with reference to FIG. **4**(*b*), include one or more recordings to be played to a consumer based on inputs received from the consumer over a telephone network. Further, the messages may be audio, visual, or audiovisual messages to be played and/or displayed to a consumer over a computer network such as the Internet **20** based on inputs received from the consumer over the computer network. Messages delivered to the consumer over the computer network may take any appropriate form, including any of the various types of targeted advertisements discussed above (e.g., banner ads, interstitial ads, real time moving videos). The targeted messages delivered over a computer network may have interactive components similar to the IVR messages, such that the message has different branching options to be played in response to receiving different inputs from the consumer over a computer network.

In step **1100** of FIG. **11**, the observed offline purchase history for each consumer is generated. This step may be implemented similar to step **500** in FIG. **5** so that master records are generated for each consumer in the purchase history database **8**.

Referring back to FIG. **11**, consumers are registered in step **1102**. Registration may occur online or offline. Online registration may be implemented similar to steps **54** through **64** in FIG. **7**. The registration process includes the registration server **14** storing registration information provided by the consumer. The registration information may include the consumer's CID, e-mail address, home address, office address, a cookie number associated with the consumer, telephone number and/or any other information that may be used to deliver targeted messages to the consumer based on his or her offline purchase history.

In step **1104**, the analytics unit **16** classifies registered consumers by assigning each consumer a purchase history classification based on his or her offline purchase history. Step **1104** may be implemented similar to step **504** in FIG. **5**. Each purchase history classification corresponds to a targeted message, and thus, each consumer is associated with a targeted message. If the targeted messages are IVR message, then they may be stored in the IVR provider **29**, for example. If the targeted messages are to be delivered over a computer network such as the Internet **20**, then the targeted messages may be stored on any computer connected to the Internet **20**, for example, the advertiser's server **18**.

In step **1106**, the analytics unit **16** assigns a unique PIN to each consumer. Accordingly, each targeted message is associated with a list of PINs for all of the consumers in the purchase history classification that corresponds to that targeted message. A record, such as the data object **460** of FIG. **4**(*b*), links the list of PINs for each purchase history classification with the corresponding targeted message, for example. Alternatively, a single PIN is assigned to a group of consumers, preferably having common features, e.g., a common purchase history classification. PINs may be generated and assigned pseudo-randomly, randomly, serially, or in any other suitable manner including those set forth in U.S. patent application Ser. No. 09/059,371, filed Apr. 14, 1998,

and entitled "Method and System for using a Frequent Shopper Card as a Phone Calling Card." U.S. patent application Ser. No. 09/059,371 and all references cited therein are incorporated herein by reference. Alternatively, PINs may be based upon an existing number, such as a telephone number or a cookie number corresponding to a consumer.

In step **1108** of FIG. **11**, the PINs are delivered to the consumers from the registration server **14** using the registration information obtained in step **1102**. The PINs may be delivered via any suitable medium, such as a computer printout at the point of sale in one of the stores **2**, **4**, **8**, e-mail, regular mail, an Internet banner, interactive TV, a personalized Web page, or a computer generated telephone message, for example. If the PINs are already known to the consumers (for example, if the PINs correspond to the consumers' telephone numbers), then the step of delivering PINs to consumers can be omitted. Each consumer is also provided with instructions for contacting a source of targeted messages or targeted message source. As shown in FIG. **1**, the targeted message source is any computer connected to the Internet **20** (e.g., advertiser's server **18**) and/or the IVR provider **29**. However, the targeted message source may be any appropriate system for storing and delivering targeted messages. Thus, the instructions for contacting the targeted message source may include a Web site or a telephone number, for example, for establishing a connection between the targeted message source and the consumer. These instructions may be provided in step **1108** or separately.

If the targeted messages are IVR messages, a consumer may use telephone **11** to dial the IVR provider **29**, and input his or her PIN over the telephone via touch tone, dual-tone multi-frequency (DTMF), voice recognition, or any other suitable method. If the PIN is the consumer's telephone number, then the IVR provider **29** may include caller identification hardware to automatically recognize the PIN as the consumer's telephone number. On the other hand, if the targeted messages are delivered to the consumer over a computer network such as the Internet **20**, the consumer uses a computer such as the first computer **10** to access a Web site identified in the instructions for contacting the targeted message source. Thus, the instructions may provide the consumer with a URL for the Web site hosted by the advertiser's server **18**. If the PIN is a cookie number previously assigned to the consumer's computer, then the cookie number may be automatically sent to the targeted message source as the PIN so that the consumer does not have to manually enter the PIN.

In step **1110**, the source of the targeted messages (e.g., IVR provider **29** or advertiser's server **18**) receives a PIN from a consumer and the targeted message (e.g., an IVR message or a real time moving video) corresponding to that PIN is initiated. If the targeted message is an interactive message, such as an IVR message or an interactive real time moving video, then the targeted message has several different variations, depending on the input from the consumer. For example, an interactive targeted message may begin by sending the following recording to the consumer: "Press 1 if you prefer Brand X over Brand Y. Press 2 otherwise." After the consumer inputs a 1 or a 2, the next recorded message that the consumer hears will depend on whether the source of the targeted messages receives a 1 or a 2 from the consumer. Alternatively, the targeted message may not have any variations, but may be a message in which the consumer is not given any branching options.

The targeted messages may include targeted advertisements, including promotional offers designed to induce the consumer to engage in a particular pattern of behavior. Thus, the value contract, discussed above with reference to FIG. **10** may be offered in an IVR message or a real time moving video. Also, different value contracts could be offered by the same interactive targeted message through different branching options, depending on which inputs are received from the consumer.

In step **1112**, the consumer receives a reward for providing his or her PIN to the targeted message source. The reward may be any of the rewards discussed above for the value contract, including points that accumulate and can be redeemed for a prize. For example, a consumer may receive 10 points each time he or she provides his or her PIN and participates in an IVR message. As another example, the rewards can be delivered as coupons appearing on a personalized Web page, Internet banner, e-mail, regular mail, etc. The targeted messages can also be used to ask asks consumers how and where they would prefer to receive and/or redeem their reward, e.g., at home by e-mail, in retail store X at a kiosk, in retail store Y at a checkout counter. Further, the rewards can be conditioned on the consumer's behavior; for example, the consumer is informed that the reward will only be received once the consumer's shopper card is presented at the checkout counter of retail store Z.

To ensure that consumers do not use the same PIN over and over again to receive a reward, each PIN is preferably only usable once. Once a PIN expires or is used, the process may return to step **1106** to assign new PINs. Alternately, old PINs can be reset by the registration server **16** so that the PINs become usable again. It is also to be noted that step **1112** may be skipped if no reward is necessary to induce consumers to receive targeted messages, or if for any other reason it is undesirable to reward the consumers. This may be the case where the consumers receive information that is valuable to them in the targeted message in step **1110**. Thus, a targeted message itself can be structured as a reward, for example, by offering the consumers a value contract or any other information that may be of value to the consumer, including a promotion or information of a discount.

Accordingly, steps **1100** through **1112** may be implemented to engage in different targeted messages with different classifications of consumers. Since the classifications are based on the offline purchase history of the consumers, the targeted messages can be targeted based on the consumers offline tastes and preferences. If the targeted messages are interactive messages, the flexibility of the interactive messages permits each different message to be tailored based on the inputs received from consumer, further enhancing the degree to which advertisements and offers can be targeted.

This invention may be conveniently implemented using a conventional general purpose computer or micro-processor programmed according to the teachings of the present invention, as will be apparent to those skilled in the computer art. Appropriate software can readily be prepared by programmers of ordinary skill based on the teachings of the present disclosure, as will be apparent to those skilled in the software art.

FIG. **12** is a schematic illustration of a computer **100** for implementing the method of the present invention. A computer **100** implements the method of the present invention, wherein the computer housing **102** houses a motherboard **104** which contains a CPU **106**, memory **108** (e.g., random access memory (RAM), dynamic ram (DRAM), static RAM (SRAM), synchronous DRAM (SDRAM), flash RAM, read-only memory (ROM), programmable ROM (PROM), eras-

able PROM (EPROM), and electrically erasable PROM (EEPROM)), and other optional special purpose logic devices (e.g., application specific integrated circuits (ASICs)) or configurable logic devices (e.g., generic array of logic (GAL) or reprogrammable field programmable gate array (FPGA)). The computer **100** also includes plural input devices (e.g., a keyboard **122** and a mouse **124**) and a display card **110** for controlling a monitor **120**. In addition, the computer system **100** further includes a floppy disk drive **114**; other removable media devices (e.g., a compact disc **119**, a tape, and a removable magneto-optical media (not shown)); and a hard disk **112**, or other fixed, high density media drives, connected using an appropriate device bus (e.g., a small computer system interface (SCSI) bus, an enhanced integrated device electronics (IDE) bus, or an ultra direct memory access (DMA) bus). Also connected to the same device bus or another device bus, the computer **100** may additionally include a compact disc reader **118**, a compact disc reader/writer unit (not shown), or a compact disc jukebox (not shown). Although compact disc **119** is shown in a CD caddy, the compact disc **119** can be inserted directly into CD-ROM drives which do not require caddies. In addition, a printer (not shown) also provides printed listings of master records, targeted ad profiles, lists of identifiers (e.g., CIDs and corresponding cookie numbers), and any other data stored and/or generated by the computer **100**.

As stated above, the system includes at least one computer readable medium or memory programmed according to the teachings of the invention and for containing data structures, tables, records, or other data described herein. Examples of computer readable media are compact discs **119**, hard disks **112**, floppy disks, tape, magneto-optical disks, PROMs (EPROM, EEPROM, Flash EPROM), DRAM, SRAM, SDRAM, etc. Stored on any one or on a combination of computer readable media, the present invention includes software for controlling both the hardware of the computer **100** and for enabling the computer **100** to interact with a human user (e.g., a consumer). Such software may include, but is not limited to, device drivers, operating systems and user applications, such as development tools. Such computer readable media further includes the computer program product of the present invention for performing all or a portion (if processing is distributed) of the processing performed in implementing the invention. The computer code devices of the present invention can be any interpreted or executable code mechanism, including but not limited to scripts, interpreters, dynamic link libraries, Java classes, and complete executable programs. Moreover, parts of the processing of the present invention may be distributed for better performance, reliability, and/or cost.

The invention may also be implemented by the preparation of application specific integrated circuits or by interconnecting an appropriate network of conventional component circuits, as will be readily apparent to those skilled in the art.

Obviously, numerous modifications and variations of the present invention are possible in light of the above teachings. For example, a consumer may provide his or her email address during registration so that targeted advertisements may be delivered to the consumer electronically via e-mail. Additionally, the consumer may register online or offline at any suitable location (such as one of the stores **2**, **4**, or **6**) by providing his or her email address and any additional information, if needed, to associate the consumer's e-mail address with the consumer's master record in the purchase history database. Further, purchase history information may be stored in one or more databases other than the purchase history database **8**. It is therefore to be understood that within the scope of the appended claims, the invention may be practiced otherwise than as specifically described herein.

We claim:

1. A method for delivering a targeted advertisement, comprising the steps of:

generating a first identifier corresponding to a first computer;

sending the first identifier to the first computer;

receiving a second identifier corresponding to a consumer from the first computer;

associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

selecting a targeted advertisement to be delivered to the consumer, based on the purchase behavior classification assigned to the consumer;

receiving from the first computer the first identifier corresponding to the first computer and associated with the observed offline purchase history of the consumer, the offline purchase history including information of an offline purchase of a consumer collected when the offline purchase transpired;

electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer;

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an updated observed offline purchase history corresponding to the second identifier; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

2. A method for delivering a targeted advertisement, comprising the steps of:

generating a first identifier corresponding to a first computer;

sending the first identifier to the first computer;

receiving a second identifier corresponding to a consumer from the first computer;

associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

selecting a targeted advertisement to be delivered to the consumer, based on the purchase behavior classification assigned to the consumer; wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established purchase behavior;

receiving from the first computer the first identifier corresponding to the first computer and associated with the

observed offline purchase history of the consumer, said purchase history including information of an offline purchase of a consumer collected when the offline purchase transpired; and

electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer;

wherein the step of electronically delivering the targeted advertisement to the consumer comprises: delivering the promotional incentive to the first computer;

wherein the method further comprises the steps of:

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an updated observed offline purchase history corresponding to the second identifier; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

3. A method for delivering a targeted advertisement, comprising the steps of:

monitoring a consumer's offline purchase at a point of sale when the offline purchase transpires;

determining, using information of the offline purchase collected during the monitoring step, a targeted advertisement to be delivered to the consumer;

electronically delivering the targeted advertisement to the consumer; wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in behavior and continuance of an established behavior; and wherein the step of electronically delivering the targeted advertisement to the consumer comprises: delivering the promotional incentive to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history, said purchase history including information of the consumer's offline purchase;

selecting the promotional incentive to be delivered, based on the purchase behavior classification assigned to the consumer;

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on the at least one selected purchase behavior cri terion and an updated observed offline purchase history, said updated purchase history including information of an additional offline purchase of the consumer; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

4. A method for delivering targeted messages, comprising the steps of:

monitoring a consumer's offline purchase at a point of sale when the purchase transpires;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and information of the offline purchase collected during the monitoring step;

assigning to the consumer a personal identification number (PIN) associated with the purchase behavior classification; and

delivering a targeted message to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the targeted message is an interactive voice response message and the step of delivering a targeted message comprises: playing the interactive voice response message over a telephone network to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the interactive voice response message is a targeted advertisement and the step of playing an interactive voice response message comprises: delivering a targeted advertisement to the consumer based on the consumer's purchase behavior classification;

wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established behavior;

wherein the step of delivering the targeted advertisement comprises: delivering the promotional incentive to the consumer;

and wherein the method further comprises the steps of:

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on the at least one selected purchase behavior criterion and an additional offline purchase of the consumer; and

assigning to the consumer another PIN associated with the updated purchase behavior classification.

5. A computer readable medium containing program instructions for execution on a computer system, which when executed by a computer, cause the computer system to perform method steps for delivering a targeted advertisement, said method comprising the steps of:

generating a first identifier corresponding to a first computer;

sending the first identifier to the first computer;

receiving a second identifier corresponding to a consumer from the first computer;

associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

selecting the targeted advertisement to be delivered, based on the purchase behavior classification assigned to the consumer;

receiving from the first computer the first identifier corresponding to the first computer and associated with the observed offline purchase history of the consumer, said purchase history including information of an offline purchase collected at a point of sale when the purchase transpired;

electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer;

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an

updated observed offline purchase history corresponding to the second identifier; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

6. A computer readable medium containing program instructions for execution on a computer system, which when executed by a computer, cause the computer system to perform method steps for delivering a targeted advertisement, said method comprising the steps of:

generating a first identifier corresponding to a first computer;

sending the first identifier to the first computer;

receiving a second identifier corresponding to a consumer from the first computer;

associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

selecting a targeted advertisement to be delivered, based on the purchase behavior classification assigned to the consumer;

receiving from the first computer the first identifier corresponding to the first computer and associated with the observed offline purchase history of the consumer, said purchase history including information of an offline purchase collected at a point of sale when the purchase transpired;

electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer; wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established purchase behavior; and wherein the step of electronically delivering the targeted advertisement to the consumer comprises: delivering the promotional incentive to the first computer;

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an updated observed offline purchase history corresponding to the second identifier; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

7. A computer readable medium containing program instructions for execution on a computer system, which when executed by a computer, cause the computer system to perform method steps for delivering a targeted advertisement, said method comprising the steps of:

monitoring a consumer's offline purchase at a point of sale when the offline purchase transpires;

determining, using information of the offline purchase collected during the monitoring step, a targeted advertisement to be delivered to the consumer;

electronically delivering the targeted advertisement to the consumer; wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in behavior and continuance of an established behavior; and wherein the step of electronically delivering the targeted advertisement to the consumer comprises: delivering the promotion to the consumer;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history, said purchase history including information of the consumer's offline purchase;

selecting the promotional incentive to be delivered, based on the purchase behavior classification assigned to the consumer;

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on the at least one selected purchase behavior criterion and an updated observed offline purchase history, said updated purchase history including information of an additional offline purchase of the consumer; and

reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

8. A computer readable medium containing program instructions for execution on a computer system, which when executed by a computer, cause the computer system to perform method steps for delivering targeted messages, said method comprising the steps of:

monitoring a consumer's offline purchase at a point of sale when the purchase transpires;

classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and using information of the offline purchase collected during the monitoring step;

assigning to the consumer a personal identification number (PIN) associated with the purchase behavior classification; and

delivering a targeted message to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the targeted message is an interactive voice response message and the step of delivering a targeted message comprises: playing the interactive voice response message over a telephone network to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the interactive voice response message is a targeted advertisement and the step of playing an interactive voice response message comprises: delivering the targeted advertisement to the consumer based on the consumer's purchase behavior classification;

wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established behavior;

wherein the step of delivering the targeted advertisement comprises: delivering the promotional incentive to the consumer;

and wherein the computer readable medium further comprises computer-executable instructions for causing the computer system to perform the steps of:

reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on

the at least one selected purchase behavior criterion and an additional offline purchase of the consumer; and

assigning to the consumer another PIN associated with the updated purchase behavior classification.

9. A system for delivering a targeted advertisement, comprising:

means for generating a first identifier corresponding to a first computer;

means for sending the first identifier to the first computer;

means for receiving a second identifier corresponding to a consumer from the first computer;

means for associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

means for classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

means for selecting a targeted advertisement to be delivered, based on the purchase behavior classification assigned to the consumer;

means for receiving from the first computer the first identifier corresponding to the first computer and associated with the observed offline purchase history of a consumer, said purchase history including information of an offline purchase of the consumer collected at a point of sale when the purchase transpired;

means for electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer;

means for reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an updated observed offline purchase history corresponding to the second identifier; and

means for reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

10. A system for delivering a targeted advertisement, comprising:

means for generating a first identifier corresponding to a first computer;

means for sending the first identifier to the first computer;

means for receiving a second identifier corresponding to a consumer from the first computer;

means for associating the first identifier with the consumer by linking the first identifier to the second identifier corresponding to the consumer;

means for classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history corresponding to the second identifier;

means for selecting the targeted advertisement to be delivered, based on the purchase behavior classification assigned to the consumer;

means for receiving from the first computer the first identifier corresponding to the first computer and associated with the observed offline purchase history of the consumer, said purchase history including information of an offline purchase of the consumer collected at a point of sale when the purchase transpired;

means for electronically delivering the targeted advertisement to the consumer at the first computer in response to receiving the first identifier from the first computer;

wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established purchase behavior; and wherein the means for electronically delivering the targeted advertisement to the consumer comprises: means for delivering the promotional incentive to the first computer;

means for reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on at least one selected purchase behavior criterion and an updated observed offline purchase history corresponding to the second identifier; and

means for reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

11. A system for delivering a targeted advertisement, comprising:

means for monitoring a consumer's offline purchase at a point of sale when the offline purchase transpires;

means for determining, using information of the offline purchase collected by the means for monitoring, a targeted advertisement to be delivered to the consumer;

means for electronically delivering the targeted advertisement to the consumer; wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in behavior and continuance of an established behavior; and wherein the means for electronically delivering the targeted advertisement to the consumer comprises: means for delivering the promotional incentive to the consumer;

means for classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and an observed offline purchase history, said purchase history including information of the consumer's offline purchase;

means for selecting the promotional incentive to be delivered, based on the purchase behavior classification assigned to the consumer;

means for reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on the at least one selected purchase behavior criterion and an updated observed offline purchase history, said updated purchase history including information of an additional offline purchase of the consumer; and

means for reselecting the targeted advertisement to be delivered, based on the updated purchase behavior classification assigned to the consumer.

12. A system for delivering targeted messages, comprising:

means for monitoring a consumer's offline purchase at a point of sale when the purchase transpires;

means for classifying the consumer by assigning to the consumer a purchase behavior classification based on at least one selected purchase behavior criterion and using information of the offline purchase collected by the means for monitoring;

means for assigning to the consumer a personal identification number (PIN) associated with the purchase behavior classification; and

means for delivering an interactive voice response message to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the targeted message is an interactive voice response message and the means for delivering a targeted message comprises: means for playing the interactive voice response message over a telephone network to the consumer in response to receiving the PIN from the consumer, based on the purchase behavior classification associated with the PIN;

wherein the interactive voice response message is a targeted advertisement and the means for playing an interactive voice response message comprises: means for delivering the targeted advertisement to the consumer based on the consumer's purchase behavior classification;

wherein the targeted advertisement is a promotional incentive for the consumer to comply with a behavioral pattern selected from the group consisting of: a predefined change in purchase behavior and continuance of an established behavior;

wherein the means for delivering the targeted advertisement comprises: means for delivering the promotional incentive to the consumer;

and wherein the system further comprises:

means for reclassifying the consumer by assigning to the consumer an updated purchase behavior classification based on the at least one selected purchase behavior criterion and an additional offline purchase of the consumer; and

means for assigning to the consumer another PIN associated with the updated purchase behavior classification.

* * * * *

US005664110A

United States Patent [19]

Green et al.

[11] Patent Number: 5,664,110

[45] Date of Patent: Sep. 2, 1997

[54] **REMOTE ORDERING SYSTEM**

[75] Inventors: **Jonathan B. Green**, Belmont; **William R. Pope**, Cambridge, both of Mass.

[73] Assignee: **Highpoint Systems, Inc.**, Belmont, Mass.

[21] Appl. No.: **351,795**

[22] Filed: **Dec. 8, 1994**

[51] **Int. Cl.**[6] **G06F 7/06**; G06F 17/30

[52] **U.S. Cl.** **705/26**; 705/1; 705/27

[58] **Field of Search** 364/401, 406, 364/408, 403; 340/825.32, 825.35; 235/379–383; 395/201, 226, 227

[56] **References Cited**

U.S. PATENT DOCUMENTS

4,654,482	3/1987	DeAngelis	379/95
4,734,858	3/1988	Schlafly	364/408
4,882,475	11/1989	Miller et al.	235/383
4,897,865	1/1990	Camuel	379/91
4,947,028	8/1990	Gorog	235/381
4,972,318	11/1990	Brown et al.	364/403
4,984,155	1/1991	Geier et al.	364/401
5,023,904	6/1991	Kaplan et al.	379/91
5,047,614	9/1991	Bianco	235/385
5,117,354	5/1992	Long et al.	364/401
5,195,130	3/1993	Weiss et al.	379/908
5,250,789	10/1993	Johnsen	235/383
5,319,542	6/1994	King, Jr. et al.	364/401

OTHER PUBLICATIONS

Fergenoff. "CD–ROM Comes home=Bell Atlantic's intelligent home of the 21st century. (home–based information services", CD–ROM News Extra, v. 1, n. 6, p. 16(4). Dec. 1993, Dialog File 148, Acc. #06795500.

"Thomas Unveils Online Purchasing Network (Thomas Publishing introduces Connects electronic corporate purchasing network for industrial products". Electronic Buyers News, p.60. Dec. 11. 1995. Dialog file 9, Acc. No. 01355145.

Bethoney. "Made to order for online catalogs (iCat's Electronic commerce suite . . .)". PC Week, vol. 13, No. 45, p.80(1). Nov. 11. 1996. Dialog file 47 Acc. No. 04634978.

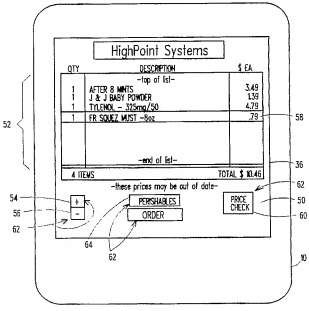
Staten. "iCat to do Net commerce. (Interactive Catalog's iCat Electronic Commerce Suite) . . . ". MacWeek, v. 10, n. 17, p.18(2). Apr. 29. 1996. Dialog file 148, Acc. No. 08633302.

Primary Examiner—Gail O. Hayes
Assistant Examiner—Frantzy Poinvil
Attorney, Agent, or Firm—Weingarten, Schurgin, Gagnebin & Hayes LLP

[57] **ABSTRACT**

A remote ordering system provides a user the ability to build and edit one or more order lists, resident in memory within a user device, and the further ability to review and manipulate a user interpretable display of the contents of such lists. A system comprising merchant stock databases, a data format/transfer computer (DFTC), and display/processor units (DPUs) (the user devices) enable creation and transmission of the order lists. Coded data read into each DPU identifies items to be added to the order lists. A DPU database contains user-discernable item information stored according to the associated coded data and is capable of learning new or updating old item information when in communication with the merchant database. Item information can be automatically or manually deleted to free DPU memory.

75 Claims, 15 Drawing Sheets



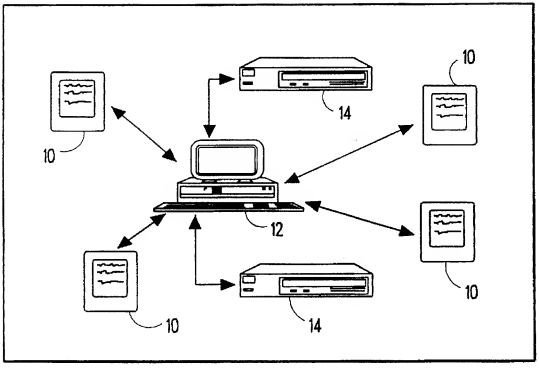


FIG. 1

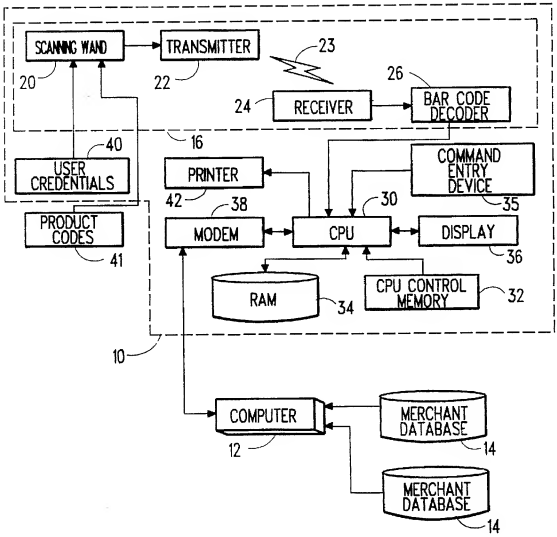

SCANNING WAND
TRANSMITTER
23
20
22
26
24
RECEIVER
BAR CODE DECODER
16
40
USER CREDENTIALS
PRINTER
COMMAND ENTRY DEVICE
42
38
30
35
PRODUCT CODES
MODEM
CPU
DISPLAY
41
36
RAM
CPU CONTROL MEMORY
34
32
10
COMPUTER
MERCHANT DATABASE
12
14
MERCHANT DATABASE
14

FIG. 2

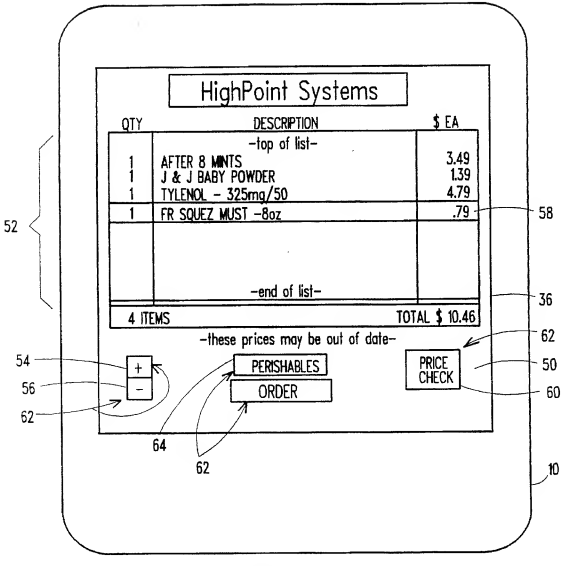

HighPoint Systems
QTY
DESCRIPTION
$ EA
-top of list-
1 AFTER 8 MINTS 3.49
1 J & J BABY POWDER 1.39
1 TYLENOL - 325mg/50 4.79
1 FR SQUEZ MUST -8oz .79
-end of list-
4 ITEMS
TOTAL $ 10.46
-these prices may be out of date-
PERISHABLES
ORDER
PRICE CHECK
52
54
56
62
64
62
58
36
62
50
60
10

FIG. 3

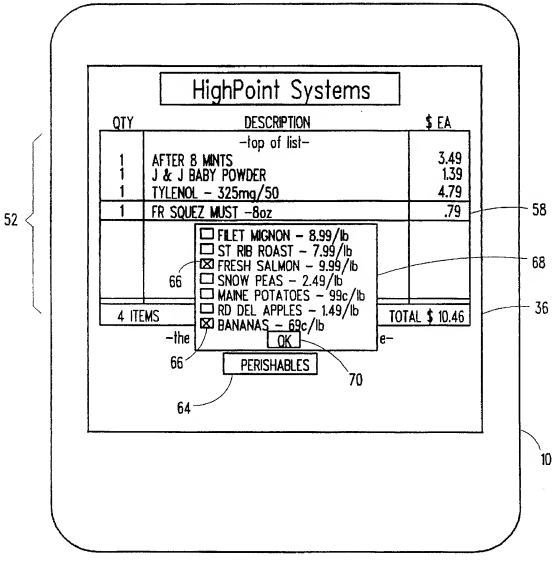

HighPoint Systems
QTY
DESCRIPTION
$ EA
-top of list-
1 AFTER 8 MINTS 3.49
1 J & J BABY POWDER 1.39
1 TYLENOL - 325mg/50 4.79
1 FR SQUEZ MUST -8oz .79
FILET MIGNON - 8.99/lb
ST RIB ROAST - 7.99/lb
FRESH SALMON - 9.99/lb
SNOW PEAS - 2.49/lb
MAINE POTATOES - 99c/lb
RD DEL APPLES - 1.49/lb
BANANAS - 69c/lb
OK
PERISHABLES
4 ITEMS
TOTAL $ 10.46
-the
e-
52
58
68
66
36
66
70
64
10

FIG. 4

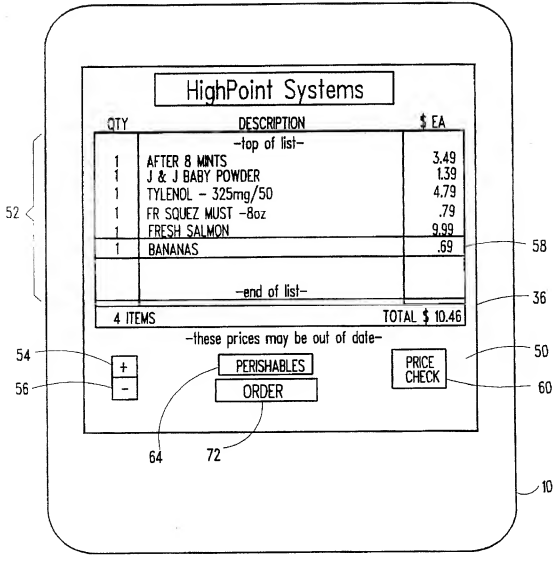

HighPoint Systems
QTY
DESCRIPTION
$ EA
-top of list-
1 AFTER 8 MINTS 3.49
1 J & J BABY POWDER 1.39
1 TYLENOL - 325mg/50 4.79
1 FR SQUEZ MUST -8oz .79
1 FRESH SALMON 9.99
1 BANANAS .69
-end of list-
4 ITEMS
TOTAL $ 10.46
-these prices may be out of date-
+
-
PERISHABLES
ORDER
PRICE CHECK
52
54
56
64
72
58
36
50
60
10

FIG. 5

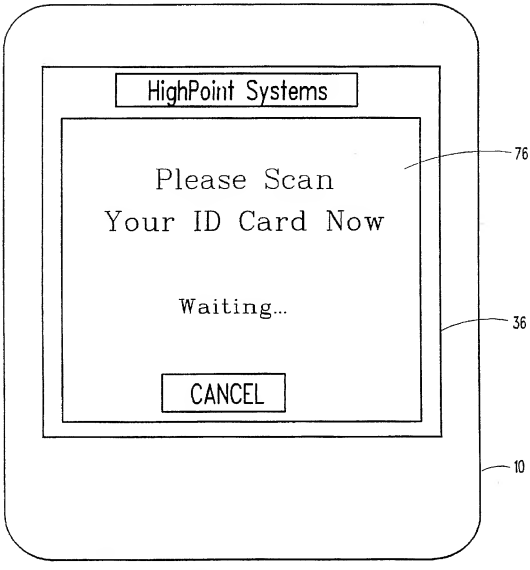

HighPoint Systems
Please Scan
Your ID Card Now
Waiting...
CANCEL
76
36
10

FIG. 6

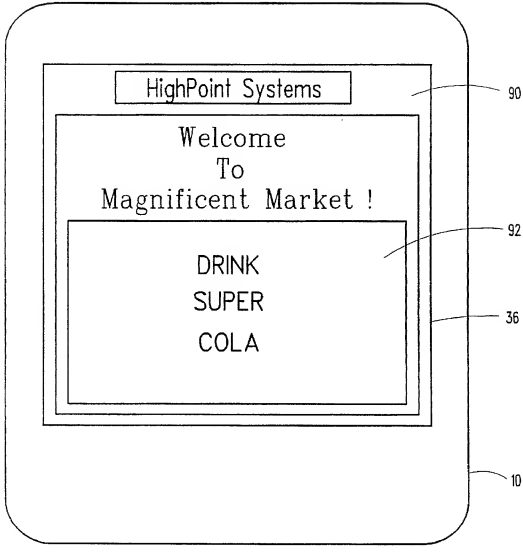

HighPoint Systems
Welcome
To
Magnificent Market !
DRINK
SUPER
COLA
90
92
36
10

FIG. 7

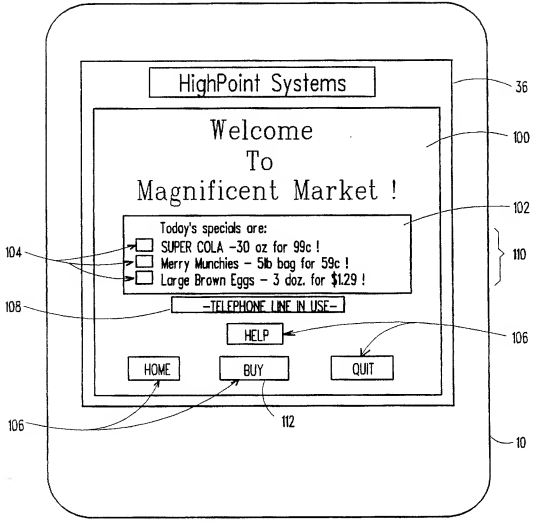

HighPoint Systems
Welcome
To
Magnificent Market !
Today's specials are:
SUPER COLA -30 oz for 99c !
Merry Munchies - 5lb bag for 59c !
Large Brown Eggs - 3 doz. for $1.29 !
-TELEPHONE LINE IN USE-
HELP
HOME
BUY
QUIT
36
100
102
104
110
108
106
106
112
10

FIG. 8

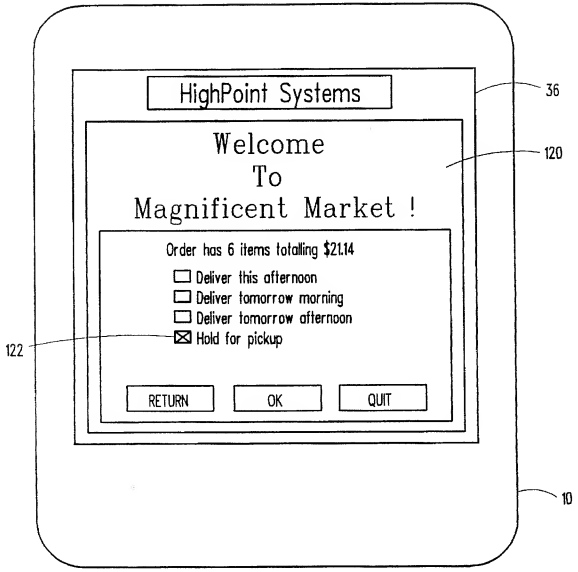

HighPoint Systems
36
Welcome
To
Magnificent Market !
120
Order has 6 items totalling $21.14
Deliver this afternoon
Deliver tomorrow morning
Deliver tomorrow afternoon
Hold for pickup
122
RETURN
OK
QUIT
10

FIG. 9

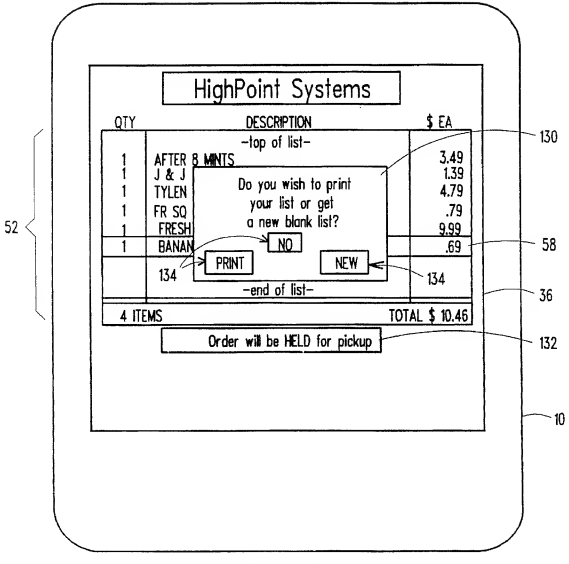

HighPoint Systems
QTY
DESCRIPTION
$ EA
-top of list-
1 AFTER 8 MINTS 3.49
1 J & J 1.39
1 TYLEN 4.79
1 FR SQ .79
1 FRESH 9.99
1 BANAN .69
Do you wish to print your list or get a new blank list?
NO
PRINT
NEW
134
134
-end of list-
4 ITEMS
TOTAL $ 10.46
Order will be HELD for pickup
52
130
58
36
132
10

FIG. 10

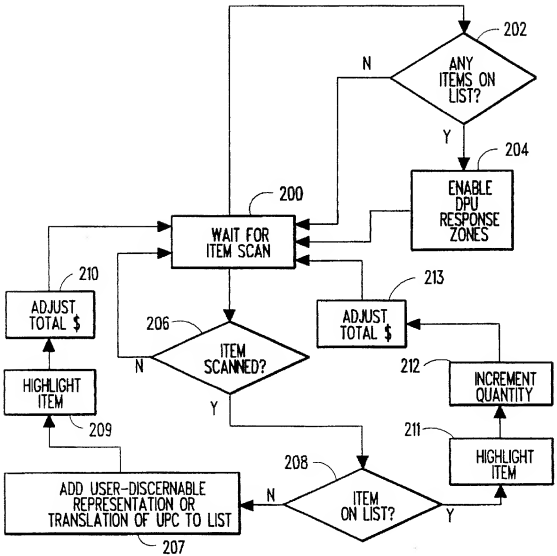

202
ANY ITEMS ON LIST?
N
Y
204
ENABLE DPU RESPONSE ZONES
200
WAIT FOR ITEM SCAN
210
ADJUST TOTAL $
206
ITEM SCANNED?
N
Y
213
ADJUST TOTAL $
212
INCREMENT QUANTITY
211
HIGHLIGHT ITEM
HIGHLIGHT ITEM
209
208
ADD USER-DISCERNABLE REPRESENTATION OR TRANSLATION OF UPC TO LIST
207
N
ITEM ON LIST?
Y

FIG. 11

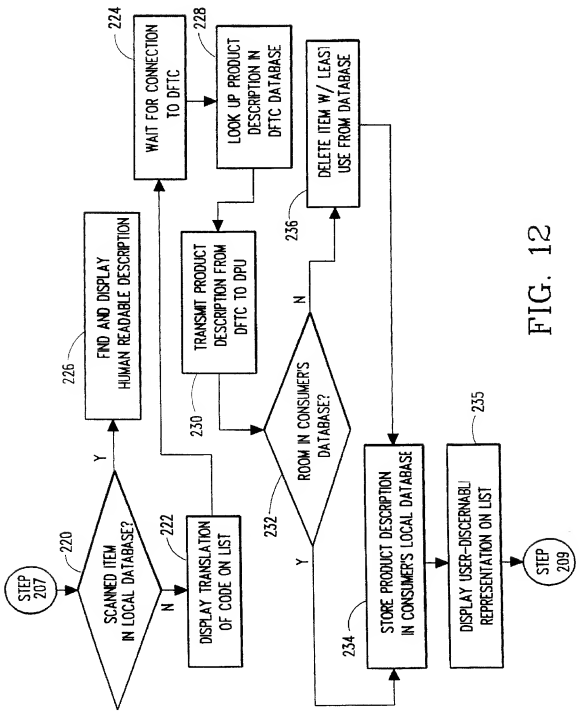

STEP 207
220
SCANNED ITEM IN LOCAL DATABASE?
Y
N
222
DISPLAY TRANSLATION OF CODE ON LIST
226
FIND AND DISPLAY HUMAN READABLE DESCRIPTION
224
WAIT FOR CONNECTION TO DFTC
228
LOOK UP PRODUCT DESCRIPTION IN DFTC DATABASE
230
TRANSMIT PRODUCT DESCRIPTION FROM DFTC TO DPU
232
ROOM IN CONSUMER'S DATABASE?
N
236
DELETE ITEM W/ LEAST USE FROM DATABASE
Y
234
STORE PRODUCT DESCRIPTION IN CONSUMER'S LOCAL DATABASE
235
DISPLAY USER-DISCERNABLE REPRESENTATION ON LIST
STEP 209

FIG. 12

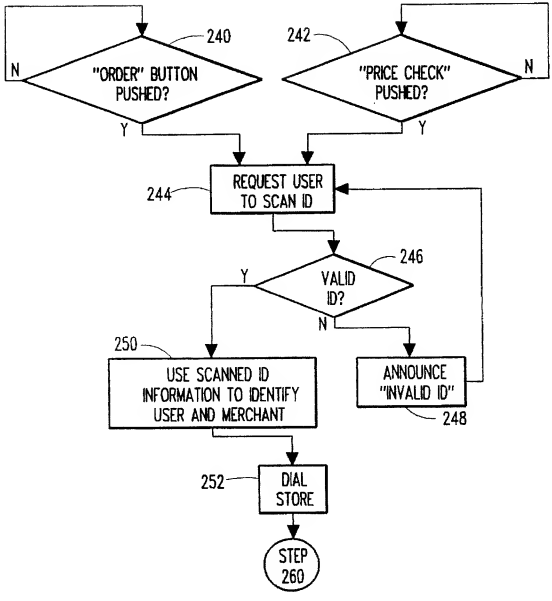

240
"ORDER" BUTTON PUSHED?
N
Y
242
"PRICE CHECK" PUSHED?
N
Y
244
REQUEST USER TO SCAN ID
246
VALID ID?
Y
N
250
USE SCANNED ID INFORMATION TO IDENTIFY USER AND MERCHANT
ANNOUNCE "INVALID ID"
248
252
DIAL STORE
STEP 260

FIG. 13

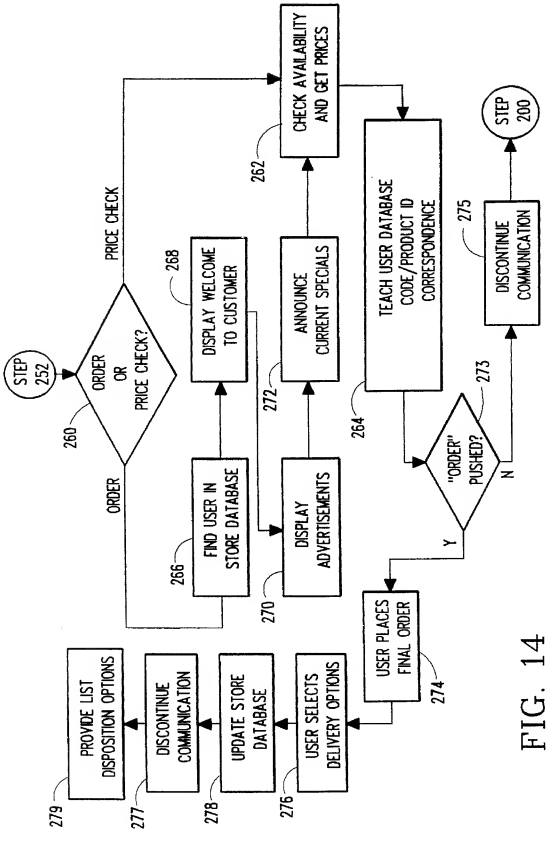

STEP 252
260
ORDER OR PRICE CHECK?
PRICE CHECK
ORDER
268
DISPLAY WELCOME TO CUSTOMER
262
CHECK AVAILABILITY AND GET PRICES
272
ANNOUNCE CURRENT SPECIALS
264
TEACH USER DATABASE CODE/PRODUCT ID CORRESPONDENCE
275
DISCONTINUE COMMUNICATION
STEP 200
266
FIND USER IN STORE DATABASE
270
DISPLAY ADVERTISEMENTS
"ORDER" PUSHED?
273
Y
N
274
USER PLACES FINAL ORDER
276
USER SELECTS DELIVERY OPTIONS
278
UPDATE STORE DATABASE
277
DISCONTINUE COMMUNICATION
279
PROVIDE LIST DISPOSITION OPTIONS

FIG. 14

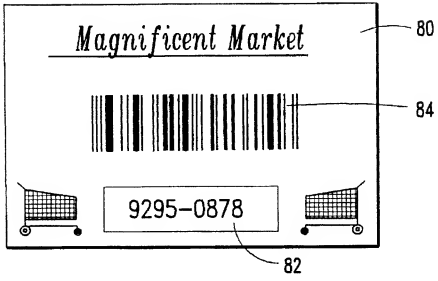


FIG. 15A

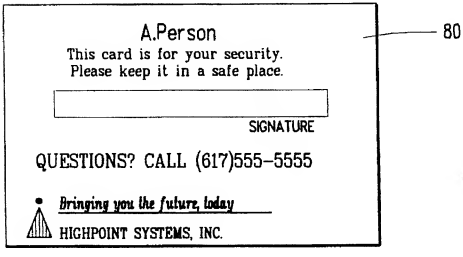


FIG. 15B

REMOTE ORDERING SYSTEM

FIELD OF THE INVENTION

The present invention relates to the field of remote ordering systems, and in particular to a remote ordering system which enables the building of a database of user-discernable product or service identification information within a user-accessible device.

BACKGROUND OF THE INVENTION

Remote ordering systems have been proposed for providing homeowners and business-persons the ability to order staple items from one or more merchants without the need to travel to a merchant location. However, such prior art systems have failed to provide the user with adequate information necessary for tracking or editing orders made or lists compiled.

Typically, prior art remote ordering systems provide some form of optical or magnetic scanner associated with a remote interface for reading coded product identification information found on product packaging. Most such systems, such as U.S. Pat. No. 4,654,482 (DeAngelis), provide an indication that a product code has been scanned, either via an audible tone or a visual indicator such as an LED. However, none of the prior art systems describes how to produce a user-interpretable description of the products placed in a list of items based on the scanned codes such as manufacturer and product name, product size, and product cost while such list is being constructed. For example, user-readable product descriptions are only provided in DeAngelis once an order list has been completed and conveyed to a merchant's order receiving apparatus, and only while connected to a merchant's order receiving apparatus.

SUMMARY OF THE INVENTION

A remote ordering system according to the present invention provides a user the ability to build and edit one or more order lists, resident in memory within a user device, and the further ability to review a user interpretable display of the contents of such lists. The present invention provides multiple merchant stock databases, a data format/transfer computer (DFTC) as an interface between customers and the merchant databases, and a user device referred to as a display/processor unit (DPU) at each of multiple customer sites for creating and transmitting order lists.

The DPU, in an illustrative embodiment, includes of a user identification code card and a data entry device providing desired item, user, and merchant data to the remainder of the DPU. To create an order list, an item code, provided by the data entry device, is checked against a DPU internal database. For instance, the item code can be provided by scanning an optical wand over a bar code. If user-discernable information corresponding to the item code, including product manufacturer, product description, and unit price, is in the DPU database, this information is displayed to the user via a DPU display. Else, the DPU communicates with the DFTC and thence to a specified merchant database to retrieve such user-discernable information, adds it to the DPU database, and updates the displayed list. In this manner, a DPU database of user-discernable product information (also referred to as user-cognizable identifiers) is created such that order lists, comprised of products or services to be ordered, can be visually reviewed, modified, and/or confirmed by the user without communication between the DPU and an associated DFTC.

Once the order list is complete, the user identification code card is provided to the data entry device. Coded information read from the card represents user name and address, merchant name and address, and other order specific information pertinent to this user and merchant, and is interpreted by the DFTC. The order list created within the DPU is processed in conformity with this coded information.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the present invention are more fully set forth below in the fully exemplary detailed description and accompanying drawings of which:

FIG. **1** is a schematic representation of the remote ordering system according to the present invention;

FIG. **2** is a further schematic representation of the system of FIG. **1**;

FIG. **3** is a view of a first screen display on a display/processor unit (DPU) of the system of FIG. **1**;

FIG. **4** is a view of a second screen display on a DPU of the system of FIG. **1**;

FIG. **5** is a view of a third screen display on a DPU of the system of FIG. **1**;

FIG. **6** is a view of a fourth screen display on a DPU of the system of FIG. **1**;

FIG. **7** is a view of a fifth screen display on a DPU of the system of FIG. **1**;

FIG. **8** is a view of a sixth screen display on a DPU of the system of FIG. **1**;

FIG. **9** is a view of a seventh screen display on a DPU of the system of FIG. **1**;

FIG. **10** is a view of a eighth screen display on a DPU of the system of FIG. **1**;

FIG. **11** is a flow chart representation of a product input function of the system of FIG. **1**;

FIG. **12** is a flow chart representation of a database update function of the system of FIG. **1**;

FIG. **13** is a flow chart representation of establishment of a communication link in the system of FIG. **1**;

FIG. **14** is a flow chart representation of an interactive session in the system of FIG. **1**;

FIG. **15**A is a first side view Of a user identification control card employed in the system of FIG. **2**; and

FIG. **15**B is a second side view of the user identification control card of FIG. **15**A.

DETAILED DESCRIPTION

A remote ordering system according to the present invention and FIG. **1** includes at least one user device referred to as a display/processor unit (DPU) **10** or a remote ordering terminal, a data format/transfer computer (DFTC) **12** (also referred to as a central processing means or a central computer), and at least one merchant database **14** (also referred to as a central inventory database). In an exemplary embodiment used in the present description, one DPU **10** is in communication with one merchant database **14** through a DFTC **12**. However, it is envisaged that each system will typically have multiple DPUs **10** and merchant databases **14**.

While a discrete piece of hardware has been identified as the merchant database **14** in FIG. **1**, it is to be understood that throughout this document the merchant database **14** refers to a database of information not having one specific physical location. That is, the merchant database **14** can be

physically located within the DFTC **12**, within another computer or memory device located at the site of the DFTC **12** and connected thereto, or within a computer or memory device at a merchant location.

As illustrated in FIG. **2**, each DPU **10** is partially comprised of a data entry device **16** which provides coded information to the rest of the DPU **10**. In the embodiment of FIG. **2**, the data entry device **16** is made up of an optical scanning wand **20** having an RF transmitter **22** in communication with an RF receiver **24**, and made up of a bar code decoder **26**. It is intended that the scanning wand be passed over some form of bar code **41**, whether printed on packaging for a desired product, in a catalog of codes, on coupons, or printed on a credit-card sized identification control card. The specific bar code employed can be Code 128, Codabar, or one of the UPC (UPC-A, UPC-E) or EAN (EAN-8, EAN-13) codes, or any other code including system specific code. In any case, the received code is interpreted by the bar code decoder **26** to provide a common representation of the coded information, such as in ASCII format.

The RF linked scanning wand provides superior portability in a light-weight package. However, a number of other suitable devices are envisaged for the data entry device **16**. Specifically, an optical, hard-wired scanning wand **20** may be employed in lieu of the wand **20**, RF transmitter **22**, RF link **23** and RF receiver **24**. Thus, the link **23** can represent a path for optical, audio, RF, IR or any other energy capable of conveying information. Further, a portable optical scanning wand **20** having a limited amount of memory may be employed to gather and store coded information within the wand **20**. This scanned information is then transferred to the remainder of the DPU **10** by the appropriate link **23**. Further alternative embodiments of the data entry device **16** of the present invention employ a standard "QWERTY" keyboard or custom keypad in communication with the remainder of the DPU **10** for manual data input, or voice-recognition circuitry or magnetic stripe input means.

In a smart terminal version of the DPU **10** shown in FIG. **2**, a central processing unit (CPU) **30** and associated CPU control memory **32** manage the DPU **10** operations. In the illustrated embodiment, the control memory **32** is read-only memory (ROM). The other memory associated with the CPU **30** in this embodiment is a random access memory (RAM) **34**. This RAM **34** can be subdivided into a sub-memory for maintenance and storage of a database of user-discernable information correlating to user-input codes (also referred to as a database memory), a submemory for maintenance and storage of custom reference lists, and a submemory for maintenance and storage of one or more active ordering lists. The custom reference lists referred to include sublists which a user may wish to recall and incorporate into an order list currently being constructed. Examples of such custom reference lists include: a) a list of perishables regularly ordered from a grocery; b) a list of office products such as staples and paper regularly ordered from a stationary supplier; and, c) a list of dairy products regularly ordered from a dairy. User-discernable information, as referred to herein, includes descriptions of products or services selected by a user, typically including manufacturer, item name or description, unit size, and unit cost. Depending upon the item (product or service) selected, other information can be displayed to the user.

Note that in alternative embodiments, the DPU **10** can have only one memory such as RAM **34**, the CPU control functions being downloaded thereto upon communication with the DFTC **12**. Further, it is envisaged in alternative embodiments that the CPU control functions are both found in ROM **32** as well as in RAM **34**. Thus, the illustrated memory configuration is but one acceptable alternative.

A further alternative configuration for the DPU **10** includes a removable media interface associated with the RAM **34**. For instance, this interface can be a CD-ROM reader, a magnetic diskette reader, a PCMCIA card interface, or any other form of interface for a removable data storage element. This configuration thus enables the DPU **10** to have a database of user-discernable information correlating to user-input codes (the database memory) which can, at least in part, be updated en masse. The RAM **34** associated with the removable media provides storage for user-discernable information not found on the removable media, and provides storage for more current information associated with certain user-input codes than that found on the removable media. Thus, references herein to "a DPU database stored within a database memory in RAM" includes, in this alternative embodiment, a DPU database stored within a database memory in RAM and in removable media associated with the DPU.

Without establishing communications between the DPU **10** and the DFTC **12**, data from the data entry device **16** (referred to as input code) to the CPU **30** is checked against a DPU **10** database stored within a database memory in RAM **34**. If user-discernable information correlating to the input code exists within the database memory in RAM **34**, the user-discernable information is added to a list of products to be ordered being constructed within the RAM **34**. Simultaneously, the user-discernable information is provided to a display **36** under the control of the CPU **30** where the information is added to the displayed list of products being ordered. The CPU **30** is in charge of creating and displaying order lists on the display **36**. Note that the user-discernable information can be presented to the user as printed text, graphic images, or a combination of both. Thus, list building, reviewing, and/or modification is done on the DPU **10** without a communications link being established between the DPU **10** and the DFTC **12**.

Once the user has completed an order list, the CPU **30** can receive commands from the user via a command entry device **35** to convey the list to a merchant. The specific steps involved will be discussed subsequently. In an illustrative embodiment of the DPU **10** according to the present invention, the command entry device **35** is a display **36** having a touch-sensitive screen. This touch sensitivity can be implemented through an IR or heat sensitive display **36** or electrically conductive grids on the display **36**. Other embodiments of the command entry device **35** for transmission of user commands include touch-responsive icons on an electro-optical display **36**, programmable buttons located on the DPU **10** housing and proximate to the display **36**, and a keyboard attached to the DPU **10**. In yet another embodiment, the DPU **10** receives user instructions via a command entry device **35** such as a mouse, light pen, trackball or remote pointing device such as an air mouse, each either in wired or wireless communication with the DPU **10**, as appropriate. Further, the same device can be used to perform the functions of both the data entry device **16** and the command entry device **35**.

In response to these user instructions, the CPU **30** can command a modem **38** to establish telephone communications, either cellular or wired, with the DFTC **12**. Alternative embodiments of the present invention can employ interactive CATV, satellite communications, or fiber-optic data transmission for the link between the DPU **10** and the DFTC **12**. The DPU **10** is used to initiate an

interactive session with the DFTC **12** after an order has been compiled within the DPU **10**. The DPU **10** can also initiate an interactive session with the DFTC **12** when identification, price or nutritional information regarding a particular product is desired by a user and is not found within a DPU **10** database.

The DFTC **12** controls the flow of information between the DPU **10** and the merchant database **14** during such an interactive session. The DFTC **12** communicates with the merchant database **14** to ascertain product availability, product identification information such as name, container size, and nutritional data, and current product price. This information is then relayed back to the DPU **10** for display to the user and for addition to or substitution within the DPU **10** database. Depending upon the actual physical location of the merchant database **14**, this communication can be a telephonic serial data transfer, a serial or parallel transfer of information over a data bus or link, or a serial transfer of information over a communications network such as the Internet. Other known communication means are envisioned.

The DFTC **12** also interprets information entered from user identification control cards **40** reflective of user and merchant identification. Typically, these identification control cards **40** provide information from which merchant name and location, user name, address and account number, payment arrangements, preferred product delivery option, and consumer profile can be determined. In alternative embodiments of the present invention, the DPU **10** has such user and merchant identification pre-stored therein, such that the user selects a merchant from a displayed menu of merchants. The appropriate account number, preferred delivery mode, etc. can then be automatically selected, or the user can choose an account number along with other appropriate parameters from another displayed menu. In any case, information identifying the user and the desired merchant, among other transaction specific information, is referred to as a transaction identifier or as identifier means.

The DFTC **12** also provides advertising to the display **36** pertinent to the merchant being accessed and potentially according to the user profile. This advertising draws the attention of the user to special sale items. An exemplary advertising screen will be discussed in conjunction with FIGS. **7** and **8**. Other information can be conveyed in addition to or in place of advertising. For instance, a message indicative of an available credit limit or past due payments can be displayed, as well as a summary of payment or delivery options selected.

As depicted in FIG. **2**, the DFTC **12** serves as an intermediary between the DPU **10** and one or more merchant databases **14**. Note that, as shown in FIG. **1**, more than one DPU **10** can be in communication with any one DFTC **12**, and thence to a plurality of merchant databases **14**. Typically, a DFTC **12** will access a merchant database **14** upon receipt of an order from a DPU **10**. The computer **12** can verify that the merchant database **14** reflects availability of a sufficient quantity of the items requested and can confirm the preferred mode of payment and order delivery, both for the user and the merchant, by searching the merchant database **14**. The DFTC **12** can also access the merchant database **14** upon receipt of a request from a DPU **10** to update the DPU database memory in RAM **34**.

Note that the communication links between an individual DPU **10** and an associated DFTC **12**, and between the DFTC **12** and a merchant database **14**, need not be concurrently established. Thus, if the communications link between the DFTC **12** and the merchant database **14** is unavailable for any reason, the DPU **10** is not tied up pending successful establishment of this link. The DFTC **12** can, as a result of periodic communications with the merchant database **14**, supply the DPU **10** with the requested information. Further, the DFTC **12** can cause an indication to be displayed on the DPU **10** that the user should attempt the operation requiring DFTC-merchant database communication again at a later time.

If the DPU **10** has never been used to order a particular item and if the DPU **10** database was not preloaded with user-discernable information relating to the particular time, the DPU **10** database stored in RAM **34** will be unable to provide the user with a user-discernable interpretation of the product identifying code and/or a most-recent per unit cost, since list building is ordinarily performed "off-line", or in the absence of DPU **10**-DFTC **12** communications. Instead, the DPU **10** can display, for instance, a numerical representation of the scanned code information. Under most circumstances, this information will be of little use to the DPU **10** user, who can command the DPU **10** to search the merchant database **14** via the DFTC **12** for user-discernable product description. In an alternative embodiment, price information can also be returned in conjunction with the user-discernable product information. As noted, the returned user-discernable information, including unit cost if desired, is stored within the DPU **10** database in the database memory within RAM **34**, and is substituted for the numerical representation on the DPU display **36**.

In a further alternative embodiment of the present remote ordering system, each DPU **10** may be issued to a user with a pre-programmed DPU database stored within RAM **34**. Such a database stored therein can include common household staple items such as milk, bread, butter, etc. for a DPU **10** to be used primarily for grocery ordering, though other items are envisaged depending upon the intended use. Thus, in addition to being delivered with an empty database in RAM **34**, a DPU **10** may come with a standard pre-programmed database in RAM **34**, a pre-programmed database in RAM **34** configured for a particular user, or a pre-programmed database in RAM **34** configured for a particular merchant.

In yet another embodiment of the present invention, if a DPU **10** user believes a price associated with a displayed product description is out-of-date, the user can command the DPU **10** to update the price in the DPU database within RAM **34** by accessing the merchant database **14** via the DFTC **12**. The merchant database **14** can indicate the current price, which the DFTC **12** returns to the DPU CPU **30** for substitution into the database in RAM **34**. The merchant database **14** can also return information on alternative products if ordered products are out of stock or are not carried by that merchant.

The steps involved in updating the DPU **10** database are further explored in conjunction with exemplary display screens and operational flow charts, as described below.

The DPU **10** can also have an associated printer **42** as illustrated in FIG. **2**. This enables a user to make a hard copy of one or more order lists prior to list deletion. The printer **42** can be housed within a DPU **10** housing, or can be a peripheral device attached to the DPU **10** housing. Other peripheral devices which can be employed with the DPU **10** include but are not limited to a magnetic memory read/write device such as a disk drive, PCMCIA cards, a magnetic stripe card reader, or a voice recognition circuit and associated hardware.

In addition to printing a processed order list, the order list can be stored within the DPU RAM **34**. Thus, as described above, custom reference lists can be created for frequently ordered items. These lists can be periodically recalled from database memory **34** by the user, edited according to the user's present needs, used as the basis for a new order, and stored anew. Alternatively, the newly modified list can be discarded, leaving the original list in memory **34**. In this manner, a number of useful lists can be created and stored within database memory **34** for subsequent retrieval and use by a user. Further, one list can serve as the basis for a number of lists, each developed according to products offered by a respective merchant.

In FIGS. **3–10**, exemplary DPU display screens are illustrated, roughly following a sequence of steps involved in creating and submitting an order list. Note that variations in the format and order of the illustrated screens is within the scope of the present invention. These figures will also be discussed in conjunction with flow charts depicted in FIG. **11–14**, in which the operation of the remote ordering system according to the present invention is mapped.

FIG. **3** illustrates a typical order entry screen **50**. It is envisaged that the DPU **10** will typically remain in an "ON" state, even when not in use, waiting for an order to be added to an open order list **52**, though minimal power will be consumed. No communications link is established between the DPU **10** and the DFTC **12** during the building of an order list. Thus, when a user determines that a particular product is needed, or will soon be needed, a user must only input a desired product identifying code such as by scanning the wand **20** across a bar code. In one embodiment of the DPU **10**, a screen saver function may be implemented which blanks the display **36** after a predetermined amount of idle time. Thus, it is preferred that the DPU **10** is "ON" and has an order list on the display **36** at an initial step **200** in FIG. **11**.

In the illustrated embodiment of FIG. **3**, once an item has been added to a current product order list **52**, response icons **62** are provided along the bottom of the display **36**, though it is understood that the icons **62** could be disposed in other locations within the display **36**. The icons **62**, also referred to as command entry devices **35**, are virtual buttons provided on the display **36** and are responsive to touch from a finger or stylus, or to light from a light wand (depending upon the embodiment of the display **36**), and in the illustrative embodiment include increment/decrement icons **54**, **56** for adjusting the listed quantity associated with a highlighted item **58**. Activation of the icons **62** is represented at steps **202** and **204** of FIG. **11**.

As illustrated in steps **206**, **207**, **208**, **209**, **210**, **211**, **212** and **213**, an item is added to the order list **52** by scanning the product code. If the item is not on the order list **52** already, a user-discernable description of the item is entered onto the bottom of the list **52** if such description exists with the database, and the description becomes the highlighted item **58**. In the alternative embodiment as described above, a unit price taken from the database in the memory **34** also appears within the order list **52**. The order cost total is then updated. Note that while not illustrated, the DPU **10** is capable of calculating applicable sales tax and adding this amount to the total cost. Flags associated with each product in the database in RAM **34** would provide an indication to the DPU **10** that the item is subject to local sales tax. Note further that if all items on the current order list do not have corresponding user-discernable descriptions and associated prices, no total will be calculated at step **210**.

An item already on the order list **52** can also become the highlighted item **58** by manipulation of arrow icons or keys (not illustrated) disposed proximate the response icons **62** or fabricated on the DPU **10** housing, or by activating the product description of the item on a touch sensitive or electro-optical display **36**. Highlighting an item already on the order list **52** as described, followed by activating either the "+" icon or the "–" icon, causes the quantity ordered to increment or decrement. Alternatively, scanning the highlighted item causes the quantity ordered to increment. Once incremented, the total cost is updated based upon the number of incremented items and the unit cost per item. This description of how a product is added to an order list **52** assumes that a user-discernable description corresponding to an input product code exists in the DPU **10** database, and is represented schematically by steps **220** and **226** of FIG. **12**.

In the case where the desired item is not in the DPU **10** database, step **207** of FIG. **11** would further include steps **220**, **222**, and **224** of FIG. **12**. Having scanned such an item, the DPU **10** provides a translation of the scanned code in place of a user-discernable product description in the display **36**. No unit price is displayed. Note also that only this translation of the scanned code is derivable from the scanned code. The translation is distinct from the user-discernable representation of the scanned product provided by the DPU **10** database, the latter being in no way directly derivable from the product code. The translation remains in the order list **52** until communication between the DPU **10**, DFTC **12**, and merchant database **14** is initiated.

Once such a DPU **10** to DFTC **12** communication has been initiated, each ordered product or service placed on the order list being compiled not having a user-discernable representation in the local DPU **10** database is scanned for in DFTC memory. The associated user-discernable representation is then returned by the DFTC **12** to the DPU **10** for storage within the DPU **10** database in RAM **34**.

In the alternative embodiment of the present invention in which unit price data is available to the user, activation of a price inquiry icon **60** also causes the DFTC **12** to return a user-discernable product description and current unit price from the merchant database **14** to the DPU display **36** for those items having a translation of the respective item code on the display **36** and not having a user-discernable product description in the DPU **10** database, as indicated in steps **228**, **230**, **232** and **234** of FIG. **12**. This product description and price information will also be added to the DPU **10** database in RAM **34**. Of course, such information cannot be supplied if the product is not found within the merchant database **14** or the DFTC **12**. If not found within the DFTC **12**, communication is initiated between the DFTC **12** and the merchant database **14** to provide such information.

In a further alternative embodiment of the ordering system according to the present invention, the user can request nutritional information on one or more items found on a current order list. In place of or in addition to the price inquiry icon **60**, the DPU **10** may provide a nutritional information icon (not shown). As with the price inquiry icon **60**, information pertaining to a highlighted product will be returned from the DFTC **12**. The user can further be provided with the ability to request nutritional information on other items on the order list at that time, or on comparable items supplied by the merchant involved in the proposed transaction.

Each time product information is updated via activation of the price inquiry icon **60** or via initiation of an order, a product information access date in the DPU **10** database associated with each item on the order list **52** is updated along with any new product identification and unit price

information provided by the merchant database **14**, as noted in step **230** of FIG. **12**. In a first embodiment, if insufficient memory space exists within the DPU database to add a new product description and associated unit price, or if a predefined maximum size for the DPU **10** database would be exceeded by adding this new information to the database, the CPU **30** determines the oldest, or least accessed, product information based on access date. This oldest information is aged out, or deleted, from the database until sufficient room exists within RAM **34** to substitute in the new product information, as indicated in steps **236** and **234** of FIG. **12**. This creation of space within RAM **34** is referred to as database "aging". Once the user-discernable information is stored within the DPU database, it can be displayed within the displayed list, as indicated by step **235** of FIG. **12**.

In another embodiment, the CPU **30** can automatically age out information based upon frequency of use. Further, products or services can be organized within classes, with each class having its own aging parameters. Alternatively, the present invention can rely upon user intervention for decisions as to which information should be deleted from memory.

Other response icons **62** include the price inquiry icon **60** in an alternative embodiment. Since the DPU internal database within RAM **34** can contains product prices as of the date of the last order or price inquiry, a user may wish to determine the most up-to-date unit prices. Activating this icon **60** initiates communication between the DPU **10** and the DFTC **12**, the latter providing the desired unit prices for all of the items on the order list **52**. A more detailed description of the steps involved in the initiation of the communication between the DPU **10** and the merchant database **14** is provided in conjunction with the discussion of FIG. **13**, below.

Another response icon **62** which can be provided to a user via the DPU display **36** is an option list icon **64**. In the embodiment illustrated in FIG. **3**, this option list icon **64** is labelled "PERISHABLES" and when activated provides a list of frequently ordered perishables taken from the DPU internal database within memory **34**. In an alternative embodiment, activation of an option list icon **64** invokes communication between the DPU **10** and the merchant database **14** via the DFTC **12**. The merchant database **14** is prompted by the DFTC **12** for an option menu, containing names of sub-menus available, provided to the user at the DPU display **36**. For instance, if the merchant is a grocery store, the option menu can include sub-menus labelled "butcher counter", "delicatessen", "fruits", "vegetables", etc. Selection of one of these sub-menu options would result in a menu of products (and associated unit prices in the alternative embodiment) appropriate to the chosen sub-menu.

In a further embodiment of the present system, the user can scan a bar code or other machine readable code, as appropriate to the data entry device **16** or command entry device **35**, in order to invoke such sub-menus. For example, the user may wish to order butter, but may not know which brand is most suited to the user's needs. By scanning a bar code labelled "butter" on a printed menu, a sub-menu similar to those described above can be displayed, providing the user with a range of butter products to choose from. Of course, this embodiment is equally applicable to other products or services, depending upon the application for the system.

In FIG. **4**, a general list of perishables has been requested. This display can be the result of activation of the option list icon **64** labelled "PERISHABLES" in FIG. **3**, and can be the result of a suggested or typical shopping list provided by either the merchant during programming of the DPU **10** or by the supplier of the DPU **10**. Alternatively, the user can create its own custom list to be displayed upon selection of the appropriate icon from an option list.

In the exemplary embodiment of FIG. **4**, the user has chosen two items from this option list **68** of perishables, including "FRESH SALMON" and "BANANAS" as indicated by an "X" in icons **66** associated with these items. Again, these icons **66** can be touch-sensitive or electro-optical. Once the user is satisfied with the selections made from this option list **68**, the "OK" icon **70** is activated and the chosen items are added to the currently active order list **52**, as shown in FIG. **5**. Note that the highlighted item **58** in the order list **52** is now the last item from the option list **68** in FIG. **4**.

Once an order list **52** is complete and a user wishes to place an order with a merchant, an "ORDER" response icon **72** is activated. Note that this icon **72** can be otherwise labelled and located. This initiates communication between the DPU **10** and the DFTC **12**, which typically has access to a number of merchant databases **14** as depicted in FIG. **2**, and as represented by step **240** in FIG. **13**. Note that the sequence of steps taken in establishing communication between the DPU **10** and the DFTC **12** is identical to the sequence of steps initiated by activation of the price inquiry icon **60** of FIG. **3**, as represented by step **242** in FIG. **13**.

In the illustrated embodiment, to determine which of multiple merchants to order from and to determine the identity of the user, the DFTC **12** causes the DPU **10** to provide a prompt screen **76** on the DPU display **36**, shown in FIG. **6**, represented by step **244** of FIG. **13**. Each user has at least one identification control card **80** for each merchant with which the user has a remote ordering account. The identification control card **80**, which carries a user number **82**, can resemble a credit card, as illustrated in FIGS. **15**A and **15**B. The identification control card **80** can additionally or alternatively carry a coded representation **84** of the user number **82**.

As noted, the user identification control card **80** represents information regarding the merchant to be interfaced with, typically including but not limited to merchant location and account number, and further represents user information such as user name and address, delivery preference, and user profile. Security is thus provided to both the merchant and the user, since only users having valid identification control cards in their possession can initiate an order and charge to a particular account. Additional security means, such as the implementation of a call-back system or use of user-entered PIN numbers, can be incorporated into the present system.

In an alternative embodiment in which DPU **10** access security is not of heightened concern, the DPU **10** can have a code stored within the DPU **10** corresponding to a user's account number, profile, etc. as well as merchant information such as telephone number and address. The desired merchant is then chosen from a submenu of merchants.

Regardless of the means for providing user and merchant information to the DPU **10** and thus to the DFTC **12**, such information is provided only in a coded format. For instance, each user has one code assigned to him or her. Merchant account numbers, user profiles, etc. are stored within the DFTC **12**, and are accessed by the user code. Similarly, each merchant has a code. All information pertaining to each merchant is similarly stored within the DFTC **12** and can be made available to the user via the DPU **10**.

The prompt screen **76** results in input of the user number **82** or the coded representation thereof **84** into the DPU **10**. In FIG. **6**, the DPU **10** is indicating that the user should pass a scanning wand **20** over the coded representation **84** of the user identification control card **80**. The CPU **30** is able to interpret the coded information provided by the identification control card **80** via the data entry device **16** to make an initial determination whether the identification control card is valid, as depicted in step **246** of FIG. **13**. If the identification control card **80** is determined to be not valid, a message to that effect is provided to the display **36** for a limited time before the prompt screen **76** is redisplayed, as in steps **248** and **244** of FIG. **13**. However, if the validity of the identification control card **80** is confirmed by the CPU **30** as represented by step **250** and **252** of FIG. **13**, the DPU **10** uses the identification control card **80** information to identify the merchant database **14** to be interfaced and communicates with the DFTC **12**, which in turn accesses the appropriate merchant database **14**.

How a merchant database **14** reacts to communication initiated by a DPU **10** depends on whether the communication is a result of a price inquiry (activation of a price inquiry icon **60**, FIG. **3**) or of an order command (activation of an order icon **72**), as shown in step **260** in FIG. **14**. As discussed, if a user is merely requesting a price inquiry (step **242**), information is requested from the identification control card **80** for identification of the proper merchant database (steps **244** and **250**, FIG. **13**). The CPU **30** then indicates to the DFTC **12** that availability and price information is being requested for the items in the order list **52** (step **252**, FIG. **13** and step **262**, FIG. **14**). The DFTC **12** searches the merchant database **14** for accurate product description information, unit price, and product availability, and returns this information to the DPU **10**. If each product on the order list **52** had previously been ordered, and therefore a user-discernable product description is already associated with the corresponding product code in the DPU database in memory **34** for each product, the relevant product descriptions and unit prices are updated, if necessary, and the access dates are updated. If a user-discernable product description is not in the DPU **10** database and the user has requested a price inquiry, such user-discernable product information, along with current unit price, is initially downloaded to the DPU **10** database. The latter step is referred to as "teaching" the DPU **10** database. This corresponds to step **264** in FIG. **14**.

Once all items in the current list have been checked for validity and updated, if necessary, the price inquiry procedure is terminated, and the DPU **10** returns to an item entry state (steps **273** and **275**, FIG. **14**).

On the other hand, if the user has indicated a desire to place an order by activating the order icon **72**, several intermediate steps are taken, as illustrated by steps **266**, **268** and **270** of FIG. **14**. The user is first identified to the merchant database **14** according to the information provided by the scanned identification control card **80**, as shown in FIG. **13**. If there is nothing barring trade with this user, a greeting screen **90** can be provided on the DPU display **36**, as illustrated in FIG. **7**. The greeting screen **90** can be customized according to the merchant, and can include general information such as hours of operation, store locations, or advertising in a portion **92** of the DPU display **36**. Alternatively, user specific information can be provided, including account status, availability of frequently ordered products, or other personalized messages. The greeting screen **90** can remain on the display **36** for a pre-programmed time, or can remain displayed until the user takes some action, including activation of a response icon similar to those in FIG. **3**.

A promotional screen **100** can be provided to the user as depicted in FIG. **8** and as represented by step **272** of FIG. **14**. This screen **100** illustrates the ability to inform the user of special promotions which the merchant is offering. As shown, a window **102** of promotional items **110** provides both information regarding the items **110**, as well the opportunity for the user to add these items **110** to the present order list **52**. Icons **104** associated with the promotional items **110** enable such order list **52** addition. Other response icons can be provided to give the user various options regarding the purchase of the promotional items **110**.

Promotional screens **110** such as the one illustrated in FIG. **8** can be the result of merchant database **14** providing the DFTC **12** with specials to be advertised for a given period. In this case, the merchant database **14** provides advertising information to the DFTC **12** on a regular, periodic basis. In another embodiment of the present system, advertising information is provided to the DFTC **12** when the DFTC **12** contacts the merchant database **14** as a result of either a price inquiry or an order command. The advertising prompted by the merchant database **14** can be either generic in nature, that is, applicable to all users, or can be customized to the individual buying patterns of the user in question.

Also shown in FIG. **8** is a reminder indication **108** which informs the user that the DPU modem **38** is presently in communication with the DFTC **12** using the user's telephone line. As with other messages provided to the DPU display **36**, this reminder indication **108** can be in reverse video, and can be blinking on and off at a rate chosen to gain the attention of the user. While not shown in other illustrative screens provided to the user during telephonic communication between the DPU **10** and the DFTC **12**, this or an analogous message may be employed somewhere on the DPU display **36**.

After the promotional screen **100**, the user can be provided with another opportunity to review the items compiled in the present order list via a screen similar to that illustrated in FIG. **5**. This is of particular use if one or more items on the list were not previously in the DPU internal database. In such case, the user would have been provided with a numeric representation of the input product code prior to communication with the merchant database **14**. After communication, a user-discernable representation of the product code would be substituted into the order list **52**, thus enabling the user to confirm an order of the item. These user-discernable representations will also be entered into the DPU database within RAM **34** for future use, as indicated by steps **262** and **264** of FIG. **14**.

Similarly, the unit price for items in the order list is updated according to current prices as provided by the merchant database **14** to the DFTC **12**, both on the DPU display **36** and in the DPU internal database in RAM **34**.

Once the order list has been reviewed and confirmed, the user can command the DPU **10** to execute the order, as in steps **273** and **274** of FIG. **14**. This can be done by user activation of a response icon **62** such as the icon **72** labelled "ORDER" in FIG. **5**, or by activation of other similarly labelled response mechanisms. The DPU modem **38** conveys the execution order to the DFTC **12**, which can then provide the user with option screens such as a delivery option screen **120**, shown in FIG. **9** and step **276** of FIG. **14**. The user is thus provided with the opportunity to specify how the ordered products are to be conveyed. In FIG. **9**, the

user has activated a response icon **122** directing that the order be held for pick-up. The order list is then provided to the merchant from the DFTC **12** telephonically via voice, in hard copy, on magnetic media, or telephonically via a modem. It is further envisaged that the order list is conveyed electronically to the merchant such that the merchant is able to update the merchant's inventory control system automatically based on the order list.

Once the user has responded to whatever option screens are provided, depending upon the configuration of the ordering system, telephonic communication between the DPU **10** and the DFTC **12** is terminated, as in step **277**. From the point of view of the user, a final step in the ordering process can be a list disposition option screen **130**, as shown in FIG. **10**. This screen **130** provides the user with the ability, through the use of response icons **134**, to print the current order list **52**, to generate a new blank order list, to return to the order list **52** just completed, or to store the order list **52** within RAM **34**, as reflected in step **279** of FIG. **14**.

In an alternative embodiment, the list disposition option screen **130** can provide the user the opportunity to store the current option order list **52** as one of several user selectable order lists. Such an alternative embodiment can further provide the user the ability to recall one of several stored order lists. An option menu can provide a textual description of stored order lists available, or such stored lists can be made available via descriptive icons.

From the point of view of the merchant database **14**, the final step in the ordering process, as reflected in step **278** of FIG. **14**, is to update the merchant database **14** to reflect the user order just processed. Thus, in addition to providing a convenient way for a user to compile and order a list of needed products, the present system enables automated maintenance of merchant inventory.

The foregoing description of the remote ordering system according to the present invention has been described with reference to an individual user ordering products, specifically groceries. It should be understood that the present system is in no way limited in product applications to a single user ordering groceries. Rather, the user can be multiple employees of a commercial customer, and the products being ordered can be regularly ordered items such as office products. Further, there is no limitation to products; the present system can also be employed to order services from a variety of sources. Examples of products and services which can be ordered using the present invention include video rental, dry cleaning and laundry, snow removal, lawn mowing, prescriptions, and overnight delivery services.

The greeting screen **90**, the promotional screen **100**, and the delivery options screen **120** have each been described as discrete screens to be sequentially provided on the DPU display **36**. However, it is understood that one or more of these screens may be combined with other displayed information in order to provide some or all of the referenced information and capabilities to the user in other combinations.

The physical embodiment of the ordering system of the present invention has been described as a DPU **10** having various user activated response icons or command entry devices **35** located within the display **36**, such as the icons **104**, **106** illustrated in FIG. **8** and the icons **134** illustrated in FIG. **10**. It has been noted that these icons can be provided as IR touch-sensitive, electrically conductive touch-sensitive, or electro-optically responsive. The function of the response icons or command entry devices **35** can also be performed by software programmable function keys disposed about the periphery of the DPU display **36**. However, in order to minimize DPU **10** unit cost and to simplify the appearance and operation of the DPU **10**, response icons such as those referenced above are preferred.

In an alternative embodiment to the DPU **10** as illustrated in and discussed with respect to FIG. **2**, the DPU **10** is a dumb terminal which must be in communication with the DFTC **12** in order to provide user-discernable representations of scanned items. Thus, the database of such representations is found within the DFTC **12**, rather than in the DPU **10** RAM **34**. In such a configuration, database updating can be executed upon scanning an item at a DPU **10**, at a regular interval with each or selected merchants, or at the time of execution of an order, price inquiry, or request for nutritional information.

In a further alternative to the embodiment described above, it is envisaged that the system of the present invention can be responsive to a bar code or other machine readable code such that a number of items are added to an order list currently being constructed. For instance, a recipe can have an associated bar code printed with it. Once scanned, the bar code is used to locate a number of products associated with the scanned code representing various ingredients needed for the preparation of the recipe. The user can then determine if any of the ingredients are on hand and can thus be removed from the list prior to commanding an order. Note that the ingredients are added to the displayed list in user-discernable format. Thus, the list of contents for each recipe is treated as an individual item by the DPU **10**, described above. If the recipe has not been "learned" by the DPU **10** database in RAM **34**, the DPU **10** will communicate with the DFTC **12** in order to learn the ingredients of the recipe. If the database is too full to learn the recipe ingredients, the database will "age-out" the earliest stored and least used item or recipe, as described above. Of course, this alternative embodiment for the present system can be applied to other products and services, depending upon the nature of the goods ordered via the DPU **10**, and is not limited to recipes.

These and other examples of the concept of the invention illustrated above are intended by way of example and the actual scope of the invention is to be determined from the following claims.

What is claimed is:

1. A remote ordering terminal for providing at least one list of at least one item or group of items to a remotely located order processing system associated with one or more merchants on each of a plurality of occasions, each item or group of items having an item code associated therewith, said remote ordering terminal comprising:

user and/or merchant identifier means;

at least one data entry device for providing said terminal with said item associated item codes and with data from said user and/or merchant identifier means;

a database unit providing a user-specific database including user-discernable item data associated with item codes for user-selected items or groups of items;

memory to provide storage for said user-specific database, said memory in communication with said at least one data entry device for storing said at least one list;

communication means for associating said memory and said order processing system upon user command for remotely accessing said order processing system over a multi-user network, for transmitting said at least one list to said order processing system using said data from said user and/or merchant identifier means, and for

receiving new and/or replacement user-discernable item data from said order processing system during association of said memory and said order processing system, said new and/or replacement user-discernable item data corresponding only to said at least one item or group of items of said at least one list;

a message display portion in communication with said memory and said user-specific database for displaying order pertinent information including said user-discernable item data from said memory; and

at least one command entry device responsive to user selection of items from said order pertinent information for assembling said at least one list and for enabling said user command, resulting in said transmitting of said at least one list to said order processing system,

wherein said at least one list is comprised of an order to be processed by said order processing system, or a provisional order list transmitted to said order processing system, transmission of either resulting in on-demand receipt of said new and/or replacement user-discernable item data within said user-specific database for said at least one item or group of items.

2. The terminal according to claim **1**, wherein said identifier means comprise data necessary for accessing said order processing system by a user including user account number.

3. The terminal according to claim **2**, wherein said identifier means are disposed within said remote ordering terminal memory.

4. The terminal according to claim **3**, wherein said identifier means are selectable by said user from a list of said identifier means stored within said remote ordering terminal memory.

5. The terminal according to claim **2**, wherein said identifier means are disposed external to and independent from said remote ordering terminal memory.

6. The terminal according to claim **1**, wherein said at least one data entry device comprises bar code detection and analysis circuitry.

7. The terminal according to claim **1**, wherein said identifier means are selectively associated with said at least one data entry device for machine recognition of said identifier means.

8. The terminal according to claim **1**, wherein said at least one data entry device is selected from a group consisting of a keyboard, a keypad, a magnetic stripe reader, and a voice recognition circuit.

9. The terminal according to claim **1**, wherein said memory is random access memory.

10. The terminal according to claim **1**, wherein said memory further stores at least one previously user-compiled list.

11. The terminal according to claim **1**, wherein said user-discernable database is stored within said memory.

12. The terminal according to claim **1**, wherein said terminal further comprises a processor in communication with said memory, said at least one data entry device, said communication means, said user-specific database, said message display portion, and said at least one data entry device.

13. The terminal according to claim **1**, wherein said user-discernable item data includes nutritional data applicable to a corresponding item code.

14. The terminal according to claim **1**, wherein said user-discernable item data includes a pictorial representation of an item having a corresponding item code.

15. The terminal according to claim **1**, wherein said order pertinent information includes promotional information provided by said order processing system to said remote ordering terminal via said communication means.

16. The terminal according to claim **1**, wherein said at least one command entry device and said message display portion collectively comprise a touch-sensitive display disposed within said remote ordering terminal.

17. The terminal according to claim **1**, wherein said at least one command entry device is selected from the group consisting of a mouse, a light pen, a trackball, and an air mouse.

18. The terminal according to claim **1**, wherein said at least one data entry device and said at least one command entry device are the same at least one device.

19. The terminal according to claim **1**, wherein said command entry device comprises at least one function key disposed within said remote ordering terminal.

20. The terminal according to claim **1**, wherein said memory comprises a removable media interface for interfacing removable media.

21. The terminal according to claim **20**, wherein said user-specific database is stored within said removable media.

22. A method for remote ordering at least one desired item by a user from one of a plurality of merchants using a system having a user device, a central computer, one of a plurality of merchant databases, and a communications link including a multi-user network, said at least one desired item having a unique identifying code associated therewith, the method comprising:

storing for a plurality of user-specific items, in an identifier database accessible at said user device for user perception at said user device, a user-cognizable identifier of said at least one item corresponding to said identifying code;

user inputting said identifying code corresponding to said at least one desired item into said user device by machine recognition of said user input identifying code;

accumulating from said identifier database selected ones of said user-cognizable identifiers corresponding to said input identifying codes in at least one list of desired items;

selectively associating a transaction identifier having user and/or merchant identifications with said user device to identify a selected merchant database and/or to identify said user to a selected merchant database;

commanding said user device to establish remote communication between said user device and said selected merchant database corresponding to said merchant identification through said central computer over said communications link including said multi-user network;

interactively updating only said selected one of said user-cognizable identifiers in said identifier database of user-specific items with current information provided by said merchant database over said communications link in response to a user action at said user device, said user action including

the communication of a provisional list of desired items transmitted to said selected merchant database for the purpose of providing said interactive updating, or

the communication of an order list of desired items transmitted to said selected merchant database for the purpose of providing said interactive updating and remote ordering said desired items comprising said order list; and

passing transaction specific information over said communications link including said identifying codes between said user device and said selected merchant database.

23. The method according to claim **22**, wherein said step of user inputting said identifying code includes scanning said identifying code with a bar code reader in communication with said user device.

24. The method according to claim **22**, wherein said step of user inputting said identifying code includes user inputting said identifying code corresponding to a plurality of unique products.

25. The method according to claim **22**, wherein said step of user inputting said identifying code by machine recognition includes the processing of a scanned bar code by bar code detection circuitry.

26. The method according to claim **22**, wherein said step of user inputting said identifying code by machine recognition includes the processing of input data from an element selected from the group consisting of a keyboard, a keypad, a magnetic stripe reader, and a voice recognition circuit.

27. The method according to claim **22**, wherein said step of accumulating from said identifier database selected ones of said user-cognizable identifiers in said at least one list further comprises the step of reviewing said at least one list including said user-cognizable identifiers by said user at said user device.

28. The method according to claim **22**, wherein said step of accumulating from said identifier database selected ones of said user-cognizable identifiers in said at least one list further comprises the step of modifying said at least one list including said user-cognizable identifiers by said user at said user device.

29. The method according to claim **22**, wherein said step of storing in an identifier database is comprised of storing in an identifier database disposed within said user device.

30. The method according to claim **22**, wherein said identifier database is disposed in conjunction with said central computer.

31. The method according to claim **22**, wherein said step of storing a user-cognizable identifier includes storing a user-readable description of an item corresponding to said identifying code.

32. The method according to claim **31**, wherein said step of storing a user-readable description includes storing a unit price.

33. The method according to claim **31**, wherein said step of storing a user-readable description includes storing nutritional data.

34. The method according to claim **22**, wherein said step of storing a user-cognizable identifier includes storing a pictorial representation of an item corresponding to said identifying code.

35. The method according to claim **22**, wherein said step of selectively associating a transaction identifier comprises selectively associating data indicative of information necessary for accessing said selected merchant database by said user including user account number.

36. The method according to claim **35**, wherein said step of selectively associating a transaction identifier includes transmitting said user and/or merchant identifications from said user device over said communications link to said merchant database via said central computer.

37. The method according to claim **36**, wherein said step of selectively associating a transaction identifier includes transmitting user and/or merchant identifications from a transaction identifier selected by said user from a list of plural transaction identifiers stored within said user device.

38. The method according to claim **22**, wherein said step of selectively associating a transaction identifier includes selectively associating a transaction identifier disposed external to and independent from said user device.

39. The method according to claim **38**, wherein said step of selectively associating a transaction identifier includes selectively associating a transaction identifier with said user device via machine recognition of said user and/or merchant identifications.

40. The method according to claim **39**, wherein said step of selectively associating a transaction identifier via machine recognition of said user and/or merchant identifications is executed by bar code detection and analysis circuitry.

41. The method according to claim **22**, wherein said step of commanding said user device comprises user establishment of said communication by selecting a user-responsive element associated with said user device.

42. The method according to claim **41**, wherein said step of user establishment of said communication comprises selecting a region on a touch-sensitive display disposed within said user device.

43. The method according to claim **41**, wherein said step of user establishment of said communication comprises selecting a function key disposed on said user device.

44. The method according to claim **22**, wherein said step of passing transaction specific information further includes passing advertising and promotional information supplied by said selected merchant database to said user device.

45. A remote ordering system for processing at least one order list of at least one user-selected item to be ordered, each said item having a corresponding item code, said system comprising:

a central inventory database;

a user-specific database of user-discernable item data corresponding to said item codes;

central processing means for providing remote communication over a multi-user network between said central inventory database and said user-specific database in response to a user action for teaching user-discernable item data received from said central inventory database to said user-specific database, for interactively updating said user-discernable item data contained within said user-specific database with replacement user-discernable item data received from said central inventory database in response to a user action, and for aging-out infrequently accessed user-discernable item data from said user-specific database;

memory means in communication with said central processing means and thus to said user-specific database for maintaining said at least one order list; and

an order device associated with said user-specific database, in communication with said central inventory database via said central processing means and said multi-user network, and responsive to user input, said order device comprising:

communication means for interfacing said order device with said central processing means;

identifier means for providing said remote ordering system with user and/or merchant information;

input means for providing said order service with said item codes corresponding to said at least one user-selected item to be ordered;

a display in communication with said memory means and said central processing means for providing order pertinent information, including said user-discernable item data, to a user; and

management means for controlling said display and said communication means, said management means responsive to said user input and said central processing means,

wherein said user-discernable item data to be taught and said replacement user-discernable item data correspond only to said at least one user-selected item to be ordered of said at least one order list and are interactively receivable as a result of said central processing means, responding to said user input at said order device, transmitting to said central inventory database said at least one order list comprising a list of items to be ordered or a provisional list of items for which updated user-discernable item data is desired.

46. The system according to claim **45**, wherein each said user-discernable item code corresponds to a plurality of unique products.

47. The system according to claim **45**, wherein each said item code is comprised of a bar code.

48. The system according to claim **47**, wherein said input means comprises a bar code reader and bar code detection circuitry.

49. The system according to claim **45**, wherein said central inventory database comprises said user-discernable item data.

50. The system according to claim **45**, wherein said central inventory database comprises promotional information to be communicated to said order device.

51. The system according to claim **45**, wherein said central inventory database is physically disposed within said central processing means.

52. The system according to claim **45**, wherein said user-specific database is physically disposed within said central processing means.

53. The system according to claim **45**, wherein said user-specific database is physically disposed within said order device.

54. The system according to claim **45**, wherein said user-discernable item data includes a user-readable description of an item corresponding to an item code.

55. The system according to claim **54**, wherein said user-readable description includes a unit price.

56. The system according to claim **54**, wherein said user-readable description includes nutritional data.

57. The system according to claim **45**, wherein said user-discernable item data includes a pictorial representation of an item corresponding to an item code.

58. The system according to claim **45**, wherein said user-discernable item data is taught to said user-specific database if said user-discernable item data has not been previously taught to said user-specific database.

59. The system according to claim **45**, wherein said user-discernable item data within said user-specific database is updated if said user-discernable item data within said user-specific database is not identical to said user-discernable item data from said central inventory database.

60. The system according to claim **45**, wherein said infrequently accessed user-discernable item data is aged out of said user-specific database when said user-specific database has reached a predetermined capacity.

61. The system according to claim **45**, wherein said central processing means further provides promotional information from said central inventory database to said user-specific database.

62. The system according to claim **45**, wherein said memory means is disposed within said order device.

63. The system according to claim **45**, wherein said memory means is disposed within said central processing means.

64. The system according to claim **45**, wherein said at least one order list further includes at least one interim list currently being compiled by a user, said at least one interim list being accessible for review and modification at said order device.

65. The system according to claim **45**, wherein said identifier means comprise data indicative of information necessary for accessing said central inventory database by a user including a user account number.

66. The system according to claim **45**, wherein said identifier means are disposed within said order device.

67. The system according to claim **66**, wherein said identifier means are selectable by said user from a list of said identifier means stored within said order device.

68. The system according to claim **45**, wherein said indentifier means are disposed external to and independent from said order device.

69. The system according to claim **68**, wherein said identifier means are selectively associated with said order device via machine recognition of said identifier means.

70. The system according to claim **69**, wherein said machine recognition of said identifier means is executed by bar code detection and analysis circuitry.

71. The system according to claim **45**, wherein said display further provides promotional information to a user.

72. The system according to claim **45**, wherein said order device further comprises at least one user-responsive element.

73. The system according to claim **72**, wherein said display is a touch-sensitive display, and

wherein said at least one user-responsive element comprises a region on said touch-sensitive display.

74. The system according to claim **72**, wherein said at least one user-responsive element comprises a function key disposed on said order device.

75. The system according to claim **72**, wherein said at least one user-responsive element comprises an external pointing device.

* * * * *